
MAT35B - L3A ALGÈBRE

Premier semestre — 2022-2023

Fiche 7: Dualité et réduction d'endomorphismes

Espace vectoriel dual

⋆ **1.** Soient E un espace vectoriel de dimension finie sur un corps $\Bbbk$, et $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E. On notera $P = \mathsf{Mat}_{\mathscr{B}\mathscr{B}'}$ la matrice de passage de la base $\mathscr{B}$ à la base $\mathscr{B}'$. Montrer que ${}^{\mathrm{t}}(P^{-1}) = \mathsf{Mat}_{\mathscr{B}^*\mathscr{B}'^*}$. En déduire que toute base de E^* est la duale d'une base de E.

Solution. On suppose que $\mathscr{B} = \{v_1, \dots, v_n\}$ et $\mathscr{B}' = \{w_1, \dots, w_n\}$, avec $n \in \mathbb{N}^*$. Alors, on peut écrire

$$v_j = \sum_{i=1}^{n} c_{i,j} w_i \tag{1}$$

pour tout $j \in [\![1,n]\!]$, où $c_{i,j} \in \Bbbk$ pour tous $i,j \in [\![1,n]\!]$. Par définition, la matrice $P = (c_{i,j})_{i,j\in[\![1,n]\!]}$ est la **matrice de passage** de la base $\mathscr{B}$ à la base $\mathscr{B}'$. On rappelle, que étant donné $v \in E$, le **vecteur de coordonnées** de v relatif à la base $\mathscr{B} = \{v_1, \dots, v_n\}$ est l'unique uplet $[v]_{\mathscr{B}} = (x_1, \dots, x_n) \in \Bbbk^n$ qui satisfait que

$$v = \sum_{j=1}^{n} x_j v_j. \tag{2}$$

Alors, (1) et (2) nous disent que

$${}^{\mathrm{t}}[v]_{\mathscr{B}'} = P.{}^{\mathrm{t}}[v]_{\mathscr{B}}, \tag{3}$$

où, étant donné $x \in \Bbbk^n$, ${}^{\mathrm{t}}x \in \Bbbk^{n\times 1}$ dénote le vecteur colonne associé au vecteur (ligne) x.

On rappelle que les **bases duales** $\mathscr{B}^* = \{v_1^*, \dots, v_n^*\}$ et $\mathscr{B}'^* = \{w_1^*, \dots, w_n^*\}$ de E^* sont données par $v_j^*(v_i) = w_j^*(w_i) = \delta_{i,j}$ pour tous $i,j \in [\![1,n]\!]$, où $\delta_{i,j} = 0$ si $i \neq j$ et $\delta_{i,i} = 1$. Soit $Q = (d_{i,j})_{i,j\in[\![1,n]\!]}$ la matrice de passage de $\mathscr{B}^*$ dans $\mathscr{B}'^*$, *i.e.*

$$v_j^* = \sum_{i=1}^{n} d_{i,j} w_i^*. \tag{4}$$

Alors,

$$\begin{aligned}\delta_{j,k} = v_j^*(v_k) &= \Big(\sum_{i=1}^{n} d_{i,j} w_i^*\Big)(v_k) = \sum_{i=1}^{n} d_{i,j} w_i^*(v_k)\\ &= \sum_{i,\ell=1}^{n} d_{i,j} c_{\ell,k} w_i^*(w_\ell) = \sum_{i,\ell=1}^{n} d_{i,j} c_{\ell,k} \delta_{i,\ell} = \sum_{i=1}^{n} d_{i,j} c_{i,k},\end{aligned}$$

ce qui nous dit que $Q = {}^{\mathrm{t}}(P^{-1})$.

Finalement, soient $\mathscr{B}' = \{w_1, \dots, w_n\}$ une base de E et $\hat{\mathscr{B}}$ une base de E^*. On considère la matrice de passage Q de $\mathscr{B}'^*$ dans $\hat{\mathscr{B}}$ et soit $P = {}^{t}(Q^{-1})$. On définit l'ensemble $\mathscr{B} = \{v_1, \dots, v_n\}$ via

$$v_j = \sum_{i=1}^{n} c_{i,j} w_i,$$

où $P = (c_{i,j})_{i,j\in[\![1,n]\!]}$. Comme Q est inversible, P aussi, ce qui implique que $\mathscr{B}$ est une base de E. En plus, $\hat{\mathscr{B}} = \mathscr{B}^*$ est la base duale de $\mathscr{B}$.

2. Soient E et F deux $\mathbb{k}$-espaces vectoriels de dimension finie, et b une forme bilinéaire sur $E \times F$. On définit les applications linéaires $\ell_b : E \to F^*$ et $r_b : F \to E^*$ via $\ell_b(x) = b(x, \cdot) \in F^*$ et $r_b(y) = b(\cdot, y) \in E^*$, respectivement, pour tous $x \in E$ et $y \in F$.

Soient $\mathscr{B} = (e_1, \dots, e_m)$ une base de E et $\mathscr{B}' = (f_1, \dots, f_n)$ une base de F. On note $\mathscr{B}^* = (e_1^*, \dots, e_m^*)$ et $\mathscr{B}'^* = (f_1^*, \dots, f_n^*)$ les bases duales, et A la matrice de coefficients $a_{i,j} = b(e_i, f_j)$ pour $i \in [\![1,m]\!]$ et $j \in [\![1,n]\!]$.

(a) Déterminer la matrice de r_b dans les bases $\mathscr{B}'$ et $\mathscr{B}^*$, et celle de ℓ_b dans les bases $\mathscr{B}$ et $\mathscr{B}'^*$.

(b) En déduire que ℓ_b est bijective, si et seulement si r_b est bijective, si et seulement si A est inversible. On dit dans ce cas que b est **non dégénérée**.

Solution. On rappelle que, étant donné une application linéaire $T : E \to F$, une base $\mathscr{B} = \{v_1, \dots, v_n\}$ de E et une base $\mathscr{B}' = \{w_1, \dots, w_m\}$ de F, on écrit

$$A(v_j) = \sum_{i=1}^{m} \alpha_{i,j} w_i, \tag{5}$$

pour tout $j \in [\![1,n]\!]$. On définit la **matrice** $[T]_{\mathscr{B}\mathscr{B}'}$ de T **associée** aux bases $\mathscr{B}$ et $\mathscr{B}'$ via $[T]_{\mathscr{B}\mathscr{B}'} = (\alpha_{i,j})_{i\in[\![1,m]\!],j\in[\![1,n]\!]}$. En plus, si $U : F \to G$ est une application linéaire et $\mathscr{B}'' = \{u_1, \dots, u_p\}$ est une base de G, alors (5) nous dit que

$$[U \circ T]_{\mathscr{B}\mathscr{B}''} = [U]_{\mathscr{B}'\mathscr{B}''}.[T]_{\mathscr{B}\mathscr{B}'}. \tag{6}$$

(a) On pose $A = (a_{i,j})_{i\in[\![1,m]\!],j\in[\![1,n]\!]}$. Noter que

$$r_b(f_j)(e_k) = \ell_b(e_k)(f_j) = b(e_k, f_j) = a_{k,j} = \sum_{i=1}^{n} a_{i,j} e_i^*(e_k) = \sum_{i=1}^{n} a_{k,i} f_i^*(f_j)$$

pour tous $j, k \in [\![1,n]\!]$, ce qui implique que

$$r_b(f_j) = \sum_{i=1}^{n} a_{i,j} e_i^* \text{ et } \ell_b(e_k) = \sum_{i=1}^{n} a_{k,i} f_i^*.$$

En conséquence, $[r_b]_{\mathscr{B}'\mathscr{B}^*} = A$ et $[\ell_b]_{\mathscr{B}\mathscr{B}'^*} = {}^{t}A$.

(b) L'identité (6) nous dit qu'une application $T : E \to F$ est bijective si et seulement si la matrice associée $[T]_{\mathscr{B}\mathscr{B}'}$ est inversible. En conséquence, ℓ_b est bijective si et seulement si A est inversible, si et seulement si r_b est bijective.

3. Soit E un espace vectoriel. On rappelle que, étant donné des parties $\Phi \subseteq E^*$ et $S \subseteq E$, on définit le **sous-espace vectoriel orthogonal** à Φ et le **sous-espace vectoriel orthogonal** à S par

$$\Phi_\perp = \{v \in E : \phi(v) = 0 \text{ pour tout } \phi \in \Phi\}$$

et

$$S^\perp = \{\phi \in E^* : \phi(v) = 0 \text{ pour tout } v \in S\},$$

respectivement.

Soient $\varphi_1, \dots, \varphi_\ell$ des formes linéaires sur un $\Bbbk$-espace vectoriel E. On note f l'application de E dans $\Bbbk^\ell$ définie par $f(x) = (\varphi_1(x), \dots, \varphi_\ell(x))$ pour tout $x \in E$ et $F = \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell)$.

(a) Montrer que la famille $\{\varphi_1, \dots, \varphi_\ell\}$ est libre si et seulement si f est surjective. **Indication :** montrer l'équivalence des négations et noter que f n'est pas surjective si et seulement si son image est contenue dans un hyperplan de $\Bbbk^\ell$.

(b) On suppose que $\{\varphi_1, \dots, \varphi_\ell\}$ est libre. Soit $(c_1, \dots, c_\ell)$ la base canonique de $\Bbbk^\ell$. D'après la question précédente, on peut choisir des antécédents $e_1, \dots, e_\ell$ de $c_1, \dots, c_\ell$ par f. Montrer que $E = F \oplus \mathsf{Vect}_\Bbbk\langle\{e_1, \dots, e_\ell\}\rangle$. En déduire que, étant donné $\psi \in E^*$, $\psi \in \mathsf{Vect}_\Bbbk\langle\{\varphi_1, \dots, \varphi_\ell\}\rangle$ si et seulement si l'on a l'inclusion $\mathsf{Ker}(\psi) \supseteq \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell)$.

(c) Soit $\Phi \subseteq E^*$ un sous-espace vectoriel de dimension finie. Montrer que l'inclusion $\Phi \subseteq (\Phi_\perp)^\perp$ est une égalité.

(d) Montrer que l'équivalence $\psi \in \langle\{\varphi_1, \dots, \varphi_\ell\}\rangle$ si et seulement si

$$\mathsf{Ker}(\psi) \supseteq \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell)$$

reste vraie même si $(\varphi_1, \dots, \varphi_\ell)$ n'est pas libre.

(e) Trouver un $\Bbbk$-espace vectoriel E et un sous-espace vectoriel Φ de E^* pour lequel l'inclusion $\Phi \subseteq (\Phi_\perp)^\perp$ est stricte.
Indication : pour $n \in \mathbb{N}$, noter φ_n l'application qui associe à un polynôme $P \in \Bbbk[X]$ le coefficient de X^n dans P, et ψ l'application qui associe $P(1)$ à un polynôme $P \in \Bbbk[X]$.

Solution.

(a) On note que f n'est pas surjective si et seulement si son image est contenue dans un hyperplan de $\Bbbk^\ell$. En effet, si $\mathsf{Img}(f) \neq \Bbbk^\ell$, on considère un élément maximal de l'ensemble

$$\{W \text{ sous-espace vectoriel } : \mathsf{Img}(f) \subseteq W \subsetneq \Bbbk^\ell\}$$

pour l'ordre donné par l'inclusion, qui nous donne un hyperplan de $\Bbbk^\ell$. En outre, on note que, étant donné un hyperplan $H \subsetneq \Bbbk^\ell$, il existe une application linéaire non nulle $\varphi : \Bbbk^\ell \to \Bbbk$ telle que $H = \mathsf{Ker}(\varphi)$, et que pour toute application linéaire (resp., non nulle) $\varphi : \Bbbk^\ell \to \Bbbk$ il existe $(\lambda_1, \dots, \lambda_\ell) \in \Bbbk^\ell$ (resp., non nul) tel que $\varphi(x_1, \dots, x_\ell) = \lambda_1 x_1 + \dots + \lambda_\ell x_\ell$, pour tout $(x_1, \dots, x_\ell) \in \Bbbk^\ell$.

En conséquence, f n'est pas surjective si et seulement s'il existe une application application linéaire non nulle $\varphi : \Bbbk^\ell \to \Bbbk$ telle que $\varphi \circ f = 0$. Si l'on suppose que φ est de la forme $\varphi(x_1, \dots, x_\ell) = \lambda_1 x_1 + \dots + \lambda_\ell x_\ell$ pour tout $(x_1, \dots, x_\ell) \in \Bbbk^\ell$, où

$(\lambda_1,\dots,\lambda_\ell) \in \Bbbk^\ell$ est non nul, on remarque que $\varphi \circ f = 0$ avec φ non nul équivaut à dire que

$$\sum_{i=1}^{\ell} \lambda_i \varphi_i = 0,$$

où $(\lambda_1,\dots,\lambda_\ell) \in \Bbbk^\ell$ est non nul, *i.e.* $\{\varphi_1,\dots,\varphi_\ell\}$ n'est pas libre. En conséquence, f n'est pas surjective si et seulement $\{\varphi_1,\dots,\varphi_\ell\}$ n'est pas libre.

(b) On remarque d'abord que $F = \mathsf{Ker}(f)$. En effet, $v \in \mathsf{Ker}(f)$ si et seulement si $f(v) = (\varphi_1(v),\dots,\varphi_\ell(v)) = \mathbf{0}_{\Bbbk^\ell}$, si et seulement si $\varphi_i(v) = 0$ pour tout $i \in [\![1,\ell]\!]$, si et seulement si $v \in \mathsf{Ker}(\varphi_i)$ pour tout $i \in [\![1,\ell]\!]$, si et seulement si $v \in \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell) = F$. Soit $g : \Bbbk^\ell \to E$ l'unique application linéaire qui envoie c_i dans e_i pour $i \in [\![1,\ell]\!]$. Alors, $\mathsf{Img}(g) = \langle\{e_1,\dots,e_\ell\}\rangle$, que l'on notera G. Noter que $f \circ g = \mathsf{id}_{\Bbbk^\ell}$.

Par ailleurs, on voit bien que $G = \langle\{e_1,\dots,e_\ell\}\rangle$ satisfait que $G \cap F = \{\mathbf{0}_E\}$, car, si $v \in G \cap F$, alors $v = \sum_{i=1}^{\ell} \lambda_i e_i$ et

$$\sum_{i=1}^{\ell} \lambda_i c_i = \sum_{i=1}^{\ell} \lambda_i f(e_i) = f(v) = \mathbf{0}_{\Bbbk^\ell}$$

nous disent que $\lambda_1 = \dots = \lambda_\ell = 0$, vu que $\{c_1,\dots,c_\ell\}$ est un ensemble libre, ce qui implique que $v = \mathbf{0}_E$. En outre, $G+F = E$, car, si $v \in E$, alors $v = (v-g(f(v)))+g(f(v))$, où $g(f(v)) \in G$ et $v-g(f(v)) \in \mathsf{Ker}(f)$, car $f(v-g(f(v))) = f(v)-f(v) = \mathbf{0}_{\Bbbk^\ell}$.

Si $\psi \in \langle\{\varphi_1,\dots,\varphi_\ell\}\rangle$, alors on peut écrire

$$\psi = \sum_{i=1}^{\ell} \lambda_i \varphi_i$$

avec $\lambda_1,\dots,\lambda_\ell \in \Bbbk$, ce qui implique que, si $v \in \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell)$, alors $\psi(v) = 0$, *i.e.* $\mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell) \subseteq \mathsf{Ker}(\psi)$. Noter que la preuve précédente de cette implication n'utilise pas l'hypothèse que $\{\varphi_1,\dots,\varphi_\ell\}$ soit libre. De façon réciproque, on suppose que $\mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell) \subseteq \mathsf{Ker}(\psi)$. On note que $\{\varphi_1|_G,\dots,\varphi_\ell|_G\}$ est la base duale de $\{e_1,\dots,e_\ell\}$ dans l'espace vectoriel G de dimension finie ℓ. On peut donc écrire $\psi|_G = \sum_{i=1}^{n} \lambda_i \varphi_i|_G$, avec $\lambda_1,\dots,\lambda_\ell \in \Bbbk$. Cela nous dit que $\omega = \psi - \sum_{i=1}^{n} \lambda_i \varphi_i \in E^*$ satisfait que $\omega|_G = 0$. En outre, $\omega|_F = \psi|_F - \sum_{i=1}^{n} \lambda_i \varphi_i|_F = 0$, car $F = \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell) \subseteq \mathsf{Ker}(\psi)$. Comme $F + G = E$, on conclut que $\omega = 0$, *i.e.* $\psi = \sum_{i=1}^{n} \lambda_i \varphi_i$. En conséquence, $\psi \in \langle\{\varphi_1,\dots,\varphi_\ell\}\rangle$.

(c) On remarque d'abord le fait élémentaire que l'inclusion $\Phi \subseteq (\Phi_\perp)^\perp$ est vraie de façon indépendante de la dimension de Φ. Soit $\{\varphi_1,\dots,\varphi_\ell\}$ une base de Φ et soit $F = \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell)$. Alors, c'est clair que $\Phi_\perp = F$, et la dernière partie de l'item précédent nous dit que $(\Phi_\perp)^\perp = \Phi$.

(d) On a déjà remarqué dans l'item (b) que l'implication directe est vraie sans l'hypothèse que $\{\varphi_1,\dots,\varphi_\ell\}$ soit libre. Pour montrer la réciproque il suffit de montrer que si $\Phi = \langle\{\varphi_1,\dots,\varphi_\ell\}\rangle$, alors

$$\Phi_\perp = \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell).$$

En effet, on suppose sans perte de généralité que $\{\varphi_1,\dots,\varphi_{\ell'}\} \subseteq \{\varphi_1,\dots,\varphi_\ell\}$ est une base de Φ. Alors $\varphi_{\ell'+1},\dots,\varphi_\ell \in \langle\{\varphi_1,\dots,\varphi_{\ell'}\}\rangle$, ce qui nous dit que $\mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_{\ell'}) \subseteq \mathsf{Ker}(\varphi_j)$ pour tout $j \in [\![\ell'+1,\ell]\!]$ et en conséquence

$$\mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_\ell) = \mathsf{Ker}(\varphi_1) \cap \dots \cap \mathsf{Ker}(\varphi_{\ell'}) = \Phi_\perp,$$

comme on a remarqué dans l'item précédent. Étant donné $\psi \in E^*$ tel que $\mathrm{Ker}(\psi) \supseteq \mathrm{Ker}(\varphi_1) \cap \ldots \cap \mathrm{Ker}(\varphi_\ell) = \mathrm{Ker}(\varphi_1) \cap \ldots \cap \mathrm{Ker}(\varphi_{\ell'})$, l'item précédent nous dit que ψ est une combinaison linéaire des éléments de $\{\varphi_1, \ldots, \varphi_{\ell'}\}$, donc *a fortiori* un combinaison linéaire des éléments de $\{\varphi_1, \ldots, \varphi_\ell\}$.

(e) Soit $E = \Bbbk[X]$ et pour $n \in \mathbb{N}$ soit $\varphi_n : E \to \Bbbk$ l'application linéaire qui associe à un polynôme $P \in \Bbbk[X]$ le coefficient de X^n dans P. On considère $\Phi = \langle\{\varphi_n : n \in \mathbb{N}\}\rangle$. Alors, $\Phi_\perp = \{0\}$ et $(\Phi_\perp)^\perp = E^*$. Par ailleurs, $\Phi \neq E^*$, car l'application linéaire $\psi : E \to \Bbbk$ qui associe $P(1)$ à un polynôme $P \in \Bbbk[X]$ n'appartient pas à Φ. En effet, si $\psi = \sum_{n=0}^{N} \lambda_n \varphi_n$, alors $\mathrm{Ker}(\psi) \supseteq \mathrm{Ker}(\varphi_0) \cap \ldots \cap \mathrm{Ker}(\varphi_N)$, ce qui est absurde car $X^{N+1} \in \mathrm{Ker}(\varphi_0) \cap \ldots \cap \mathrm{Ker}(\varphi_N)$ mais $X^{N+1} \notin \mathrm{Ker}(\psi)$.

4. Soient E un $\Bbbk$-espace vectoriel F, G deux sous-espaces vectoriels de E.

(a) Montrer que $F = (F^\perp)_\perp$.
Indication : si $x \in E \setminus F$, utiliser un supplémentaire de $F + \Bbbk.x$ dans E pour construire une forme linéaire nulle sur F mais pas en x.

(b) Montrer que F est de codimension finie si et seulement si F est une intersection finie d'hyperplans de E. De combien d'hyperplans a-t-on besoin ?

(c) Montrer que $(F + G)^\perp = F^\perp \cap G^\perp$.

(d) Montrer que $(F \cap G)^\perp \supseteq F^\perp + G^\perp$. Qu'en déduit-on si E est de dimension finie ?

(e) On suppose que E est de dimension finie. Soit $(e_1, \ldots, e_p)$ une base de F, qu'on complète en une base $(e_1, \ldots, e_n)$ une base de E. En déduire une base de $F^\perp$.

Solution.

(a) On remarque d'abord que l'inclusion $F \subseteq (F^\perp)_\perp$ est immédiate des définitions. Si $F \subsetneq (F^\perp)_\perp$, soit $v \in (F^\perp)_\perp \setminus F$. Alors, comme $v \in E \setminus F$, il existe une application linéaire $f : E \to \Bbbk$ telle que $f(w) = 0$ pour tout $w \in F$ et $f(v) = 1$. En effet, si $\mathscr{B}$ est une base de F, $\mathscr{B} \cup \{v\}$ est un ensemble libre qui peut se compléter en un base $\mathscr{B} \cup \{v\} \cup \mathscr{B}'$, et on définit l'unique application linéaire $f : E \to \Bbbk$ qui satisfait $f(w) = 0$ pour tout $w \in \mathscr{B} \cup \mathscr{B}'$ et $f(v) = 1$. Par ailleurs, l'application linéaire f précédente nous donne une contradiction, car dans ce cas $v \notin (F^\perp)_\perp$. En conséquence, $F = (F^\perp)_\perp$.

(b) On remarque d'abord que, étant donné un espace vectoriel E et des sous-espaces $F, H \subseteq E$ avec $\mathrm{dim}(E/H) = 1$, alors $\mathrm{dim}(F/(F \cap H)) \in \{0, 1\}$, *i.e.* $F \subseteq H$ ou $F \cap H$ a codimension 1 dans F. En effet, les deuxième théorème d'isomorphisme nous dit que

$$\frac{F}{F \cap H} \simeq \frac{F + H}{H} \subseteq \frac{E}{H},$$

ce qui implique que $\mathrm{dim}(F/(F \cap H)) \in \{0, 1\}$. Un argument immédiat par récurrence nous dit que, si $H_1, \ldots, H_r \subseteq E$ sont des sous-espaces de codimension 1 (*i.e.* hyperplans), alors $H_1 \cap \cdots \cap H_r$ a codimension inférieur ou égal à r. En conséquence, l'intersection finie de sous-espaces de codimension 1 a codimension finie. De façon réciproque, si $F \subseteq E$ est un sous-espace de codimension finie d, il existe un isomorphisme d'espaces vectoriels $f : E/F \to \Bbbk^d$. On considère la projection canonique $\pi_F : E \to E/F$ et, pour $i[\![1, d]\!]$, $\pi_i : \Bbbk^d \to \Bbbk$ la projection sur la i-ème coordonnée. Soit $\varphi_i : E \to \Bbbk$ la composition $\varphi_i = \pi_i \circ f \circ \pi_F$ et $H_i = \mathrm{Ker}(\varphi_i)$, pour $i[\![1, d]\!]$. C'est clair que H_i est un sous-espace vectoriel de codimension 1, vu que φ_i est surjectif et induit un isomorphisme $\bar{\varphi}_i : E/H_i \to \Bbbk$, et que $H_1 \cap \cdots \cap H_d = F$. On remarque l'on a besoin d'au moins $d = \mathrm{dim}(E/F)$ sous-espaces vectoriels de codimension 1 dans l'intersection précédente.

(c) On remarque d'abord le résultat immédiat suivant : si $F_1 \subseteq F_2 \subseteq E$ sont des sous-espaces, alors $F_2^{\perp} \subseteq F_1^{\perp}$. En conséquence, comme $F \subseteq F+G$ et $G \subseteq F+G$, on conclut que $(F+G)^{\perp} \subseteq F^{\perp}$ et $(F+G)^{\perp} \subseteq G^{\perp}$, ce qui implique que $(F+G)^{\perp} \subseteq F^{\perp} \cap G^{\perp}$. En outre, si $\varphi \in F^{\perp} \cap G^{\perp}$, alors $\varphi(v) = 0$ et $\varphi(w) = 0$ pour tous $v \in F$ et $w \in G$, ce qui implique que $\varphi(v+w) = 0$ pour tous $v \in F$ et $w \in G$. En conséquence, $\varphi \in (F+G)^{\perp}$ et $(F+G)^{\perp} = F^{\perp} \cap G^{\perp}$.

(d) Comme $F \cap G \subseteq F$ et $F \cap G \subseteq G$, on conclut que $F^{\perp} \subseteq (F \cap G)^{\perp}$ et $G^{\perp} \subseteq (F \cap G)^{\perp}$, ce qui implique que $F^{\perp} + G^{\perp} \subseteq (F \cap G)^{\perp}$, comme on voulait démontrer.

Soit $\iota_E : E \to (E^*)^* = E^{**}$ l'application linéaire donnée par $\iota_E(v)(\varphi) = \varphi(v)$, pour $v \in E$ et $\varphi \in E^*$. C'est clair que l'application ι_E est injective, ce qui nous dit que, si E a dimension finie, alors ι_E est un isomorphisme, car dans ce cas $\dim(E) = \dim(E^*) = \dim(E^{**})$. Si E a dimension finie et $\Phi \subseteq E^*$, on remarque alors le résultat direct

$$\iota_E(\Phi_{\perp}) = \Phi^{\perp}. \tag{7}$$

L'item précédent pour $\Phi, \Psi \subseteq E^*$ avec E de dimension finie nous dit que $(\Phi + \Psi)^{\perp} = \Phi^{\perp} \cap \Psi^{\perp}$, ce qui implique que

$$\Phi_{\perp} \cap \Psi_{\perp} = \iota_E^{-1}(\Phi^{\perp}) \cap \iota_E^{-1}(\Psi^{\perp}) = \iota_E^{-1}\big((\Phi+\Psi)^{\perp}\big) = (\Phi+\Psi)_{\perp}, \tag{8}$$

où l'on a utilisé (7).

On suppose encore que E a dimension finie, ce qui implique que E^* a aussi dimension finie, et soient $F, G \subseteq E$ des sous-espaces. D'après le premier item de cet exercice et l'item (c) de l'exercice **3**, il existe des uniques sous-espaces $\Phi, \Psi \subseteq E^*$ tels que $F = \Phi_{\perp}$ et $G = \Psi_{\perp}$, ce qui nous dit aussi que $F^{\perp} = \Phi$ et $G^{\perp} = \Psi$. En plus, les mêmes raisons nous disent que $F^{\perp} + G^{\perp} = (F \cap G)^{\perp}$ si et seulement si $(F^{\perp} + G^{\perp})_{\perp} = F \cap G$, ce qui équivaut à (8), comme on voulait démontrer.

(e) On voit bien que $(e_{p+1}, \dots, e_n)$ est une base de $F^{\perp}$.

De façon plus générale, si F est un sous-espace vectoriel d'un espace vectoriel E, alors l'application duale ${}^{t}i : E^* \to F^*$ de l'inclusion $i : F \to E$ est surjective, car toute application linéaire $\varphi : F \to \Bbbk$ admet un prolongement linéaire $\hat{\varphi} : E \to \Bbbk$, *i.e.* $\hat{\varphi} \circ i = \varphi$. En outre, le noyau de ${}^{t}i$ est précisément $F^{\perp}$, ce qui nous dit que ${}^{t}i$ induit un isomorphisme linéaire ${}^{t}\bar{i} : E^*/F^{\perp} \to F^*$. En particulier, si F est dimension finie d, $F^{\perp}$ a codimension d dans E^*.

5. Soient E un $\Bbbk$-espace vectoriel et $u \in \mathsf{L}(E)$.

(a) Soient F un sous-espace vectoriel de E. Montrer que F est stable par u si et seulement si $F^{\perp}$ est stable par ${}^{t}u$.
Indication : la démonstration par équivalences est possible, en utilisant les égalités $F = (F^{\perp})_{\perp}$.

(b) On suppose que E est de dimension finie. Soit Φ un sous-espace vectoriel de E^*. Montrer que Φ est stable par ${}^{t}u$ si et seulement si $\Phi_{\perp}$ est stable par u.

(c) Soit φ une forme linéaire non nulle sur E. Montrer que l'hyperplan donné par $\mathsf{Ker}(\varphi)$ est stable par u si et seulement φ est un vecteur propre de l'endomorphisme ${}^{t}u$.

Solution.

(*a*) On remarque que ${}^{t}u(\varphi)(v) = \varphi(u(v))$, pour tous $v \in E$ et $\varphi \in E^*$. En conséquence, si F est stable par u, alors, étant donné $\varphi \in F^{\perp}$, ${}^{t}u(\varphi)(v) = \varphi(u(v)) = 0$ pour tout $v \in F$, ce qui nous dit que ${}^{t}u(\varphi) \in F^{\perp}$. De façon réciproque, si $F^{\perp}$ est stable par ${}^{t}u$, alors, étant donné $v \in F$, $\varphi(u(v)) = {}^{t}u(\varphi)(v) = 0$ pour tout $\varphi \in F^{\perp}$, ce qui nous dit que $u(v) \in (F^{\perp})_{\perp} = F$.

(*b*) Comme E est de dimension finie, d'après les exercices **3** et **4**, il existe un unique sous-espace vectoriel $F \subseteq E$ tel que $F^{\perp} = \Phi$ et $\Phi_{\perp} = F$. D'après l'item précédent, $\Phi = F^{\perp}$ est stable par ${}^{t}u$ si et seulement si $\Phi_{\perp} = F$ est stable par u.

(*c*) Si φ est un vecteur propre de l'endomorphisme ${}^{t}u$, alors il existe $\lambda \in \Bbbk$ tel que ${}^{t}u(\varphi) = \lambda\varphi$. Alors, si $v \in \mathsf{Ker}(\varphi)$, $0 = \lambda\varphi(v) = {}^{t}u(\varphi)(v) = \varphi(u(v))$ nous dit que nous dit que $u(v) \in \mathsf{Ker}(\varphi)$, ce qui implique que $\mathsf{Ker}(\varphi)$ est stable par u.

Avant de continues, on remarque que, si deux fonctionnelles linéaires non nulles $\varphi, \psi : E \to \Bbbk$ d'un espace vectoriel sur $\Bbbk$ ont le même noyau H, il existe $\lambda \in \Bbbk^*$ tel que $\varphi = \lambda\psi$. En effet, dans ce cas φ et ψ induisent $\bar{\varphi}, \bar{\psi} : E/H \to \Bbbk$ respectivement, qui sont de isomorphismes et qui satisfont $\bar{\varphi} \circ \pi = \varphi$ et $\bar{\psi} \circ \pi = \psi$, où $\pi : E \to E/H$ est la projection canonique. Comme, étant deux isomorphismes d'un espace vectoriel de dimension 1, il sont colinéaires, il existe $\lambda \in \Bbbk^*$ tel que $\bar{\varphi} = \lambda\bar{\psi}$. Si l'on considère la composition de π avec l'identité précédente on conclut que $\varphi = \lambda\psi$.

Si $\mathsf{Ker}(\varphi)$ est stable par u, alors ${}^{t}u(\varphi)(v) = \varphi(u(v)) = 0$ pour tout $v \in \mathsf{Ker}(\varphi)$, ce qui implique que $\mathsf{Ker}({}^{t}u(\varphi)) \supseteq \mathsf{Ker}(\varphi)$. Comme le noyau d'une fonctionnelle linéaire non nulle a codimension 1, on a que $\mathsf{Ker}({}^{t}u(\varphi)) = \mathsf{Ker}(\varphi)$ ou $\mathsf{Ker}({}^{t}u(\varphi)) = E$. Dans le dernier cas, ${}^{t}u(\varphi) = 0 = 0\varphi$, tandis que dans le premier cas il existe $\lambda \in \Bbbk^*$ tel que ${}^{t}u(\varphi) = \lambda\varphi$. En conséquence, φ est un vecteur propre de l'endomorphisme ${}^{t}u$.

6. Soient E un $\mathbb{R}$-espace vectoriel de dimension finie et C un convexe fermé de E. À toute forme linéaire non nulle ϕ sur E et à tout réel β, on associe le demi-espace fermé $D_{\phi,\beta} = \{x \in E : \phi(x) \leq \beta\}$ et l'hyperplan affine $H_{\phi,\beta} = \{x \in E : \phi(x) = \beta\}$.

(*a*) Montrer que $D_{\phi,\beta}$ est une partie convexe de E. Quelle est sa frontière ?

(*b*) Montrer que C est l'intersection de demi-espaces fermés qui le contiennent. **Indication :** munir E d'un produit scalaire $\langle\cdot,\cdot\rangle$. Si $x \in E \setminus C$ et $C \neq \emptyset$, introduire la forme linéaire $\langle x - p_C(x), \cdot\rangle$, où $p_C(x)$ est la projection de x sur C.

(*c*) Un point $c \in C$ est dit **extrémal** dans C si $C \setminus \{c\}$ est convexe. Montrer que c est extrémal si et et seulement si, étant donnés $a, b \in C$, $(a + b)/2 = c$ implique $a = b = c$.

(*d*) Soit $c \in C$. Montrer que s'il existe une forme linéaire non nulle ϕ sur E telle que $\phi(x) < \phi(c)$ pour tout $x \in C \setminus \{c\}$, alors c est extrémal dans C.

(*e*) Dans cette question, on suppose que C est une intersection finie des demi-espaces fermés D_{ϕ_i,β_i} pour $i \in [\![1, m]\!]$. Étant donné $c \in C$, on définit l'ensemble $I_c = \{i \in [\![1, m]\!] : \phi_i(c) = \beta_i\}$. Montrer que $c \in C$ est extrémal dans C si et seulement si $(\phi_i)_{i \in I_c}$ engendre E^*.

(*f*) Déterminer les points extrémaux du polyèdre de $\mathbb{R}^2$ défini par les inéquations $x_1 \geq 0$, $x_2 \geq 0$, $x_1 + 2x_2 \leq 3$ et $2x_1 + x_2 \leq 3$.

Solution. Dans cet exercice on considère que E est muni d'un produit scalaire $\langle\cdot,\cdot\rangle$. La norme associée sera notée $||\cdot||$.

(*a*) Soient $v, w \in D_{\phi,\beta}$, *i.e.* $\phi(v), \phi(w) \leq \beta$. Alors,

$$\phi(tv + (1-t)w) = t\phi(v) + (1-t)\phi(w) \leq t\beta + (1-t)\beta = \beta,$$

pour tout $t \in [0,1]$. En conséquence $D_{\phi,\beta}$ est convexe.

La frontière $\partial D_{\phi,\beta}$ de $D_{\phi,\beta}$ est clairement $H_{\phi,\beta}$. En effet, si $\phi(v) < \beta$, la continuité de ϕ nous dit qu'il existe $r > 0$ tel que $\phi(w) < \beta$ pour tout $w \in B(v,r) = \{w \in E : ||w-v|| < r\}$, ce qui implique que $v \in D^{\circ}_{\phi,\beta}$. En outre, si $\phi(v) = \beta$, on prend $u \in E$ tel que $\phi(u) = 1$, ce qui existe vu que ϕ est une forme linéaire non nulle. Alors $v + \epsilon u \in D_{\phi,\beta}$ pour tout $\epsilon \leq 0$ mais $v + \epsilon u \notin D_{\phi,\beta}$ pour tout $\epsilon > 0$. Comme $v + \epsilon u$ converge vers v quand ϵ tend vers 0, on conclut que $v \in \partial D_{\phi,\beta}$.

(*b*) Soit $\mathscr{C} = \{H \subseteq E : H$ demi-espaces fermés et $C \subseteq H\}$. C'est clair que $\cap_{H\in\mathscr{C}} H \supseteq C$, vu que $H \subseteq C$ pour tout $H \in \mathscr{C}$. Pour montrer l'autre inclusion, il suffit de prouver que, si $x \in E \setminus C$, alors il existe $H \in \mathscr{C}$ tel que $x \notin H$. Si $C = \emptyset$, c'est immédiat. On suppose désormais $C \neq \emptyset$. Soit $y \in C$ est la projection de x sur C, *i.e.* $||y-x|| = \inf\{||z-x|| : z \in C\}$. Comme C est fermé et non vide et E est de dimension finie, y existe, alors que la convexité de C nous dit que y est unique. En plus, $y \neq x$, car $x \notin C$. On considère la forme linéaire $\varphi(v) = \langle x-y, v\rangle$, pour tout $v \in E$. Noter que $\varphi(x) = \langle x-y, x\rangle > \langle x-y, y\rangle = \varphi(y)$, car $\varphi(x) - \varphi(y) = ||x-y|| > 0$, ce qui nous dit que $x \notin H_{\varphi,\langle x-y,y\rangle}$. En plus, $\langle x-y, y\rangle \geq \langle x-y, v\rangle$ pour tout $v \in C$, car $||x-v|| \geq ||x-y||$ pour tout $v \in C$ et

$$||x-y||^2 = ||x-v||^2 + ||v-y||^2 + 2\langle x-v, v-y\rangle$$

impliquent $\langle x-v, v-y\rangle \leq 0$. En conséquence, $C \subseteq H_{\varphi,\langle x-y,y\rangle}$. On conclut que $H_{\varphi,\langle x-y,y\rangle} \in \mathscr{C}$, et $x \notin H_{\varphi,\langle x-y,y\rangle}$.

(*c*) Soit $c \in C$ est extrémal dans C et soient $a, b \in C$ tels que $(a+b)/2 = c$. On procédera par l'absurde et on suppose sans perte de généralité que $a \neq c$. Alors, comme $a+b = 2c$, $b \neq c$ aussi. Comme $C \setminus \{c\}$ est convexe et $a, b \in C \setminus \{c\}$, alors $(a+b)/2 = c \in C \setminus \{c\}$, ce qui est absurde. En conséquence, $a = b = c$.

De façon réciproque, on suppose que c vérifie que, étant donnés $a', b' \in C$, $(a'+b')/2 = c$ implique $a' = b' = c$. On remarque d'abord que c vérifie que, étant donnés $a, b \in C$ et $t \in [0,1]$, $ta + (1-t)b = c$ implique $a = b = c$. En effet, si $t = 1/2$ c'est clair, si $0 \leq t < 1/2$ on utilise la propriété vérifiée par c pour $a' = 2ta + (1-2t)b$ et $b' = b$, et si $1 \geq t > 1/2$ on utilise la propriété vérifiée par c pour $a' = a$ et $b' = (2t-1)a + 2(1-t)b$. On va montrer que $C \setminus \{c\}$ est convexe. Soient $a, b \in C \setminus \{c\}$. Si $t \in [0,1]$, alors $ta + (1-t)b \in C$, vu que C est convexe. Si $ta + (1-t)b = c$, alors $a = b = c$, ce qui est absurde. En conséquence, $ta + (1-t)b \in C \setminus \{c\}$, comme on voulait démontrer.

(*d*) Soient $a, b \in C$ tels que $(a+b)/2 = c$. On suppose que $a \neq c$ ou $b \neq c$. Alors, $2\phi(c) = \phi(a) + \phi(b) < \phi(c) + \phi(c) = 2\phi(c)$, ce qui est absurde. En conséquence, $a = b = c$, et c est extrémal dans C.

(*e*) On remarque d'abord le fait élémentaire qu'une famille $(\psi_j)_{j\in J}$ engendre E^* si et seulement si, étant donné $v, w \in E$, $\psi_j(v) = \psi_j(w)$ pour tout $j \in J$, alors $v = w$.

Soit $c \in C$. On suppose que $(\phi_i)_{i\in I_c}$ engendre E^*. Soient $a, b \in C$ tels que $(a+b)/2 = c$, ce qui nous dit que $\phi_i(a) + \phi_i(b) = 2\phi_i(c)$ pour tout $i \in I_c$. Comme $C \subseteq D_{\phi_i,\beta_i}$ pour tout $i \in I_c$ et $\phi_i(c) = \beta_i$, $\phi_i(a) + \phi_i(b) = 2\phi_i(c)$ implique que $\phi_i(a) = \phi_i(b) = \phi_i(c) = \beta_i$ pour tout $i \in I_c$. D'après la propriété équivalente rappelée ci-dessus pour $(\phi_i)_{i\in I_c}$, on conclut que $a = b = c$, ce qui nous dit que c est extrémal pour C.

De façon réciproque, soit $c \in C$ tel que $(\phi_i)_{i\in I_c}$ n'engendre pas E^* pour $c \in C$ fixe. Alors, il existe $v \in E$ tel que $\phi_i(v) = 0$ pour tout $i \in I_c$. En particulier, $\phi_i(c + \epsilon v) = \beta_i$

pour tout $i \in I_c$ et $\epsilon \in \mathbb{R}$. En outre, comme $c \in C$, $\phi_i(c) < \beta_i$ pour tout $i \in I \setminus I_c$, ce qui implique qu'il existe $\epsilon_0 > 0$ tel que $\phi_i(c + \epsilon v) < \beta_i$ pour tout $i \in I \setminus I_c$ et $|\epsilon| \leq \epsilon_0$. On conclut que $c + \epsilon v \in \cap_{i \in I} D_{\phi_i, \beta_i} = C$ pour $|\epsilon| \leq \epsilon_0$. Cela implique que $c = ((c + \epsilon_0) + (c - \epsilon_0))/2$, ce qui nous dit que c n'est pas extrémal pour C.

(*f*) En appliquant l'item précédent on voit bien que les points extrémaux du polyèdre $C \subseteq \mathbb{R}^2$ défini par les inéquations $x_1 \geq 0$, $x_2 \geq 0$, $x_1 + 2x_2 \leq 3$ et $2x_1 + x_2 \leq 3$ sont $(0,0)$, $(0,3/2)$, $(3/2,0)$ et $(1,1)$.

Dual de l'espace vectoriel de matrices⋆

⋆ **7.** Soient $\Bbbk$ un corps et $n \in \mathbb{N}^*$. Pour $A \in \mathsf{M}_n(\Bbbk)$, on note ϕ_A la forme linéaire sur $\mathsf{M}_n(\Bbbk)$ définie par $\phi_A(M) = \mathsf{Tr}(AM)$ pour $M \in \mathsf{M}_n(\Bbbk)$.

(*a*) Calculer $\phi_{{}^{t}A}(M)$ en fonction des coefficients de A et de M.

(*b*) Montrer que l'application $A \mapsto \phi_A$ est un isomorphisme de $\mathsf{M}_n(\Bbbk)$ vers $\mathsf{M}_n(\Bbbk)^*$ et que la forme bilinéaire b sur $\mathsf{M}_n(\Bbbk)$ définie par $b(M,N) = \mathsf{Tr}(MN)$ est non dégénérée.

(*c*) Quelles sont les formes linéaires sur $\mathsf{M}_n(\Bbbk)$ vérifiant $\phi(MN) = \phi(NM)$ pour tout M et N dans $\mathsf{M}_n(\Bbbk)$?

Solution.

(*a*) On écrira $A = (a_{i,j})_{i,j \in [\![1,n]\!]}$ et $M = (m_{i,j})_{i,j \in [\![1,n]\!]}$. Soit $E_{i,j} \in \mathsf{M}_n(\Bbbk)$ la matrice dont le coefficient dans la ligne i' et colonne j' est $\delta_{i,i'}\delta_{j,j'}$ pour tout $i', j' \in [\![1,n]\!]$. Noter que $E_{i,j}E_{k,\ell} = \delta_{j,k}E_{i,\ell}$, pour $i,j,k,\ell \in [\![1,n]\!]$. En outre, $A = \sum_{i,j=1}^n a_{i,j}E_{i,j}$ et $M = \sum_{i,j=1}^n m_{i,j}E_{i,j}$. Alors,

$$\begin{aligned}\phi_{{}^{t}A}(M) &= \sum_{k,\ell=1}^n m_{k,\ell}\phi_{{}^{t}A}(E_{k,\ell}) = \sum_{k,\ell=1}^n m_{k,\ell}\,\mathsf{Tr}(AE_{k,\ell}) \\ &= \sum_{i,j,k,\ell=1}^n a_{j,i}m_{k,\ell}\,\mathsf{Tr}(E_{i,j}E_{k,\ell}) = \sum_{i,j,k,\ell=1}^n a_{j,i}m_{k,\ell}\delta_{j,k}\,\mathsf{Tr}(E_{i,\ell}) \\ &= \sum_{i,j,k,\ell=1}^n a_{j,i}m_{k,\ell}\delta_{j,k}\delta_{i,\ell} = \sum_{i,j=1}^n a_{j,i}m_{i,j}.\end{aligned}$$

(*b*) Soit $\varphi_{i,j} : \mathsf{M}_n(\Bbbk) \to \Bbbk$ l'application linéaire qui associe $a_{i,j}$ à $A = (a_{i,j})_{i,j \in [\![1,n]\!]}$, pour $i,j \in [\![1,n]\!]$. Alors, $\{\varphi_{i,j} : i,j \in [\![1,n]\!]\}$ est une base de $\mathsf{M}_n(\Bbbk)^*$. L'item précédent nous dit que $\phi_{E_{j,i}} = \varphi_{i,j}$ pour tout $i,j \in [\![1,n]\!]$, ce qui implique que l'application $\mathsf{M}_n(\Bbbk) \to \mathsf{M}_n(\Bbbk)^*$ qui associe ϕ_A à A est un isomorphisme. Comme l'application précédente coïncide avec $\flat_b$, où b est la forme bilinéaire $b(M,N) = \mathsf{Tr}(MN)$, on conclut que b es non dégénérée.

(*c*) On affirme d'abord que le **commutateur** $[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)]$ de l'anneau $\mathsf{M}_n(\Bbbk)$, donné par l'espace vectoriel engendré par

$$\{AB - BA : A, B \in \mathsf{M}_n(\Bbbk)\},$$

coïncide avec $\{A \in \mathsf{M}_n(\Bbbk) : \mathsf{Tr}(A) = 0\}$. En effet, l'inclusion $[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)] \subseteq \{A \in \mathsf{M}_n(\Bbbk) : \mathsf{Tr}(A) = 0\}$ est une conséquence de l'identité $\mathsf{Tr}(AB) = \mathsf{Tr}(BA)$ pour tous $A, B \in \mathsf{M}_n(\Bbbk)$. Pour l'autre inclusion $[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)] \supseteq \{A \in \mathsf{M}_n(\Bbbk) : \mathsf{Tr}(A) = 0\}$, on utilise que $E_{i,j}E_{k,\ell} - E_{k,\ell}E_{i,j} = \delta_{j,k}E_{i,\ell} - \delta_{i,\ell}E_{k,j}$, pour $i, j, k, \ell \in [\![1, n]\!]$. En conséquence, $[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)] = \{A \in \mathsf{M}_n(\Bbbk) : \mathsf{Tr}(A) = 0\}$. Comme l'application linéaire $\mathsf{Tr} : \mathsf{M}_n(\Bbbk) \to \Bbbk$ est surjective, elle induit un isomorphisme $\mathsf{Tr} : \mathsf{M}_n(\Bbbk)/[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)] \to \Bbbk$, ce qui implique que $[\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)]$ a codimension 1 dans $\mathsf{M}_n(\Bbbk)$.

On remarque aussi que, si deux fonctionnelles linéaires non nulles $\varphi, \psi : E \to \Bbbk$ d'un espace vectoriel sur $\Bbbk$ ont le même noyau H, il existe $\lambda \in \Bbbk^*$ tel que $\varphi = \lambda\psi$. En effet, dans ce cas φ et ψ induisent $\bar{\varphi}, \bar{\psi} : E/H \to \Bbbk$ respectivement, qui sont de isomorphismes et qui satisfont $\bar{\varphi} \circ \pi = \varphi$ et $\bar{\psi} \circ \pi = \psi$, où $\pi : E \to E/H$ est la projection canonique. Comme, étant deux isomorphismes d'un espace vectoriel de dimension 1, il sont colinéaires, il existe $\lambda \in \Bbbk^*$ tel que $\bar{\varphi} = \lambda\bar{\psi}$. Si l'on considère la composition de π avec l'identité précédente on conclut que $\varphi = \lambda\psi$.

Or, une application linéaire $\phi : \mathsf{M}_n(\Bbbk) \to \Bbbk$ satisfait $\phi(MN) = \phi(NM)$ pour tout M et N dans $\mathsf{M}_n(\Bbbk)$ si et seulement si $\mathsf{Ker}(\phi) \subseteq [\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)]$. Si $\phi \neq 0$, cela nous dit que $\mathsf{Ker}(\phi) = [\mathsf{M}_n(\Bbbk), \mathsf{M}_n(\Bbbk)]$, ce qui implique que ϕ est un multiple de Tr. Si $\phi = 0$, c'est clair que ϕ est un multiple de Tr. En conséquence, $\phi : \mathsf{M}_n(\Bbbk) \to \Bbbk$ satisfait $\phi(MN) = \phi(NM)$ pour tout M et N dans $\mathsf{M}_n(\Bbbk)$ si et seulement si ϕ est un multiple de Tr.

Double dual d'un espace vectoriel*

* **8.** Soit E un $\Bbbk$-espace vectoriel. On note $\iota_E : E \to E^{**} = (E^*)^*$ l'application donnée par $\iota_E(x)(\varphi) = \varphi(x)$ pour tous $x \in E$ et $\varphi \in E^*$. Montrer que pour tout $u \in \mathsf{L}(E)$, ${}^{\mathsf{t}}({}^{\mathsf{t}}u) \circ \iota_E = \iota_E \circ u$. En déduire que si E est de dimension finie, ${}^{\mathsf{t}}({}^{\mathsf{t}}u) = \iota_E \circ u \circ \iota_E^{-1}$.

Solution. La définition de l'application transposée nous dit que

$$\big({}^{\mathsf{t}}({}^{\mathsf{t}}u) \circ \iota_E\big)(x)(\varphi) = {}^{\mathsf{t}}({}^{\mathsf{t}}u)\big(\iota_E(x)\big)(\varphi) = \iota_E(x)({}^{\mathsf{t}}u(\varphi)) = {}^{\mathsf{t}}u(\varphi)(x) = \varphi\big(u(x)\big) = \iota_E\big(u(x)\big)(\varphi)$$

pour tous $x \in E$ et φ, ce qui implique que $({}^{\mathsf{t}}({}^{\mathsf{t}}u) \circ \iota_E)(x) = \iota_E(u(x)) = (\iota_E \circ u)(x)$ pour tout $x \in E$, ce qui nous donne ${}^{\mathsf{t}}({}^{\mathsf{t}}u) \circ \iota_E = \iota_E \circ u$. Comme on a remarqué dans l'exercice **4**, (d), si E est de dimension finie, ι_E est un isomorphisme. Dans ce cas, l'identité prouvé est équivalente à ${}^{\mathsf{t}}({}^{\mathsf{t}}u) = \iota_E \circ u \circ \iota_E^{-1}$.

Polynômes et endomorphismes

9. Soit $\Bbbk, \mathbb{K}$ deux corps avec $\Bbbk \subseteq \mathbb{K}$ et soit $A \in \mathsf{M}_n(\Bbbk)$. On rappelle que le **polynôme minimal** $\mu_{A,\mathbb{K}}$ de A dans $\mathbb{K}[X]$ est le générateur unitaire de l'idéal

$$I_{A,\mathbb{K}} = \big\{P \in \mathbb{K}[X] : P(A) = \mathbf{0}_{\mathsf{M}_n(\mathbb{K})}\big\}$$

de $\mathbb{K}[X]$, où $\mathbf{0}_{\mathsf{M}_n(\mathbb{K})}$ désigne la matrice nulle de $\mathsf{M}_n(\mathbb{K})$. Montrer que $\mu_{A,\mathbb{R}} = \mu_{A,\mathbb{C}}$ pour $A \in \mathsf{M}_n(\mathbb{R})$.

Solution. On note d'abord que dans la situation général $\Bbbk \subseteq \mathbb{K}$ et $A \in \mathsf{M}_n(\Bbbk)$, on a que $\mu_{A,\mathbb{K}}$ divise $\mu_{A,\Bbbk}$ dans $\mathbb{K}[X]$. En effet, comme $\mu_{A,\Bbbk} \in \Bbbk[X] \subseteq \mathbb{K}[X]$ et $\mu_{A,\Bbbk}(A) = \mathbf{0}_{\mathsf{M}_n(\Bbbk)} = \mathbf{0}_{\mathsf{M}_n(\mathbb{K})}$, $\mu_{A,\Bbbk} \in I_{A,\mathbb{K}}$, ce qui démontre le résultat. En particulier, $\mu_{A,\mathbb{C}}$ divise $\mu_{A,\mathbb{R}}$ dans $\mathbb{C}[X]$.

On affirme en outre que, si $\Bbbk = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$, alors $\mu_{A,\mathbb{C}} \in \mathbb{R}[X]$. Avant de le démontrer, on introduit la notation suivante. Si $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$, on notera $\bar{P} = \sum_{i=0}^{d} \bar{a}_i X^i \in \mathbb{C}[X]$ le polynôme dont les coefficients sont les conjugués de ceux de P. Or, comme $\mu_{A,\mathbb{C}} \in \mathbb{C}[X]$ est unitaire alors $\bar{\mu}_{A,\mathbb{C}} \in \mathbb{C}[X]$ est unitaire aussi, ce qui implique que le degré de $\mu_{A,\mathbb{C}} - \bar{\mu}_{A,\mathbb{C}}$ est strictement inférieur au degré de $\mu_{A,\mathbb{C}}$. Comme

$$(\mu_{A,\mathbb{C}} - \bar{\mu}_{A,\mathbb{C}})(A) = \mu_{A,\mathbb{C}}(A) - \bar{\mu}_{A,\mathbb{C}}(A) = \mu_{A,\mathbb{C}}(A) - \overline{\mu_{A,\mathbb{C}}(A)} = \mathbf{0}_{\mathsf{M}_n(\mathbb{K})} - \mathbf{0}_{\mathsf{M}_n(\mathbb{K})} = \mathbf{0}_{\mathsf{M}_n(\mathbb{K})},$$

on conclut que $\mu_{A,\mathbb{C}} - \bar{\mu}_{A,\mathbb{C}} = \mathbf{0}_{\mathbb{C}[X]}$, *i.e.* $\mu_{A,\mathbb{C}} = \bar{\mu}_{A,\mathbb{C}}$, ce qui nous dit que $\mu_{A,\mathbb{C}} \in \mathbb{R}[X]$. Cela nous dit que $\mu_{A,\mathbb{C}} \in I_{A,\mathbb{R}}$, ce qui implique que $\mu_{A,\mathbb{R}}$ divise $\mu_{A,\mathbb{C}}$ dans $\mathbb{C}[X]$. Comme $\mu_{A,\mathbb{C}}$ et $\mu_{A,\mathbb{R}}$ sont polynômes unitaires, on conclut que $\mu_{A,\mathbb{R}} = \mu_{A,\mathbb{C}}$.

10. Trouver deux matrices carrées non semblables de même polynôme minimal et de même polynôme caractéristique.

Solution. On considère les matrices

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

dans $\mathsf{M}_4(\mathbb{R})$. C'est clair que $\chi_A = \chi_B = X^4$ et $\mu_{A,\mathbb{R}} = \mu_{B,\mathbb{R}} = X^2$, vu que $A^2 = B^2 = \mathbf{0}_{\mathsf{M}_4(\mathbb{R})}$ mais A et B ne sont pas matrices nulles. En outre, A et B ne sont pas semblables, *i.e.* il n'existe pas de matrice $P \in \mathsf{M}_4(\mathbb{R})$ inversible telle que $A = PBP^{-1}$. En effet, si A et B étaient pas semblables, alors $\mathsf{Ker}(A)$ et $\mathsf{Ker}(B)$ auraient la même dimension. Par contre, on voit bien que $\mathsf{dim}(\mathsf{Ker}(A)) = 2$ et $\mathsf{dim}(\mathsf{Ker}(B)) = 3$, ce qui nous dit que A et B ne sont pas semblables.

11. Soient $\Bbbk$ un corps, E un $\Bbbk$-espace vectoriel, $f \in \mathsf{L}(E)$ un endomorphisme linéaire, et P, Q deux polynômes de $\Bbbk[X]$. On pose

$$D = \mathsf{PGCD}(P, Q) \text{ et } M = \mathsf{PPCM}(P, Q).$$

Montrer que

$$\mathsf{Ker}\big(D(f)\big) = \mathsf{Ker}\big(P(f)\big) \cap \mathsf{Ker}\big(Q(f)\big) \text{ et } \mathsf{Ker}\big(M(f)\big) = \mathsf{Ker}\big(P(f)\big) + \mathsf{Ker}\big(Q(f)\big).$$

Solution. On note d'abord que, étant donné $R, S \in \Bbbk[X]$ tel que $R|S$, alors $\mathsf{Ker}(R(f)) \subseteq \mathsf{Ker}(S(f))$. En effet, comme R divise S dans $\Bbbk[X]$, il existe $T \in \Bbbk[X]$ tel que $S = T.R$, ce qui nous dit que $S(f) = T(f) \circ R(f)$ et en particulier $S(f)(v) = T(f)(R(f)(v))$ pour tout $v \in E$. Si $v \in \mathsf{Ker}(R(f))$, on trouve alors $S(f)(v) = T(f)(\mathbf{0}_E) = \mathbf{0}_E$, *i.e.* $v \in \mathsf{Ker}(S(f))$.

Comme $D|P$ et $D|P$, alors $\mathsf{Ker}(D(f)) \subseteq \mathsf{Ker}(P(f))$ et $\mathsf{Ker}(D(f)) \subseteq \mathsf{Ker}(Q(f))$, ce qui nous dit que

$$\mathsf{Ker}\big(D(f)\big) \subseteq \mathsf{Ker}\big(P(f)\big) \cap \mathsf{Ker}\big(Q(f)\big).$$

De façon analogue, comme $P|M$ et $Q|M$, alors $\mathsf{Ker}(P(f)) \subseteq \mathsf{Ker}(M(f))$ et $\mathsf{Ker}(Q(f)) \subseteq \mathsf{Ker}(M(f))$, ce qui nous dit que

$$\mathsf{Ker}\big(P(f)\big) + \mathsf{Ker}\big(Q(f)\big) \subseteq \mathsf{Ker}\big(M(f)\big).$$

Il suffit de montrer les autres inclusions. Pour cela, on remarque d'abord qu'il existe $R, S \in \Bbbk[X]$ tels que $D = RP + SQ$, ce qui implique que $D(f) = R(f) \circ P(f) + S(f) \circ Q(f)$. Alors, si $v \in \mathsf{Ker}(P(f)) \cap \mathsf{Ker}(Q(f))$,

$$D(f)(v) = R(f)(P(f)(v)) + S(f)(Q(f)(v)) = R(f)(\mathbf{0}_E) + S(f)(\mathbf{0}_E) = \mathbf{0}_E + \mathbf{0}_E = \mathbf{0}_E,$$

i.e. $v \in \mathsf{Ker}(D(f))$, ce qui montre la première identité demandée. Finalement, soit $\hat{P} = P/D \in \Bbbk[X]$ et $\hat{Q} = Q/D \in \Bbbk[X]$. Comme $\hat{P}$ et $\hat{Q}$ sont premiers entre eux, alors il existe $R, S \in \Bbbk[X]$ tels que $1 = \hat{Q}R + \hat{P}S$, ce qui implique que $\mathsf{id}_E = \hat{Q}(f) \circ R(f) + \hat{P}(f) \circ S(f)$, ce qui implique que $v = \hat{Q}(f)(R(f)(v)) + \hat{P}(f)(S(f)(v))$ pour tout $v \in E$. En plus, si $v \in \mathsf{Ker}(M(f))$, $\hat{Q}(f)(R(f)(v)) \in \mathsf{Ker}(P(f))$ et $\hat{P}(f)(S(f)(v)) \in \mathsf{Ker}(Q(f))$, vu que

$$\begin{aligned} P(f)\Big(\hat{Q}(f)\big(R(f)(v)\big)\Big) &= (P.\hat{Q})(f)\big(R(f)(v)\big) = M(f)\big(R(f)(v)\big) = R(f)\big(M(f)(v)\big) \\ &= R(f)(\mathbf{0}_E) = \mathbf{0}_E \end{aligned}$$

et

$$\begin{aligned} Q(f)\Big(\hat{P}(f)\big(S(f)(v)\big)\Big) &= (Q.\hat{P})(f)\big(S(f)(v)\big) = M(f)\big(S(f)(v)\big) = S(f)\big(M(f)(v)\big) \\ &= S(f)(\mathbf{0}_E) = \mathbf{0}_E, \end{aligned}$$

ce qui implique que $v \in \mathsf{Ker}(P(f)) + \mathsf{Ker}(Q(f))$, comme on voulait démontrer.

Réduction d'endomorphismes

12. Soient $\Bbbk$ un corps, E un $\Bbbk$-espace vectoriel de dimension n et $u \in \mathsf{L}(E)$ un endomorphisme linéaire. On rappelle que, étant donné $v \in E$, le sous-espace vectoriel

$$E_{u,v} = \big\{P(u)(v) : P \in \Bbbk[X]\big\} = \mathsf{Vect}_{\Bbbk}\Big\langle \big\{u^k(v) : k \in \mathbb{N}\big\}\Big\rangle$$

est appelé le **sous-espace cyclique associé** à v. On notera $I_{u,v}$ le noyau de l'application linéaire $\mathsf{ev}_{u,v} : \Bbbk[X] \to E$ définie par $\mathsf{ev}_{u,v}(P) = P(u)(v)$ pour tout $P \in \Bbbk[X]$.

(a) Montrer que $u(E_{u,v}) \subseteq E_{u,v}$ pour tout $v \in E$.

(b) Montrer que $I_{u,v}$ est un idéal de $\Bbbk[X]$ non réduit à $\{0\}$. Le **polynôme minimal** de u en v est le générateur unitaire $\mu_{u,v}$ de cet idéal.

(c) Soit d le degré de $\mu_{u,v}$. Montrer que $(v, u(v), \dots, u^{d-1}(v))$ est une base de $E_{u,v}$. Quelle est la dimension de $E_{u,v}$?

(d) Soit $u_v : E_{u,v} \to E_{u,v}$ l'endomorphisme linéaire donné par la restriction $u|_{E_{u,v}}$ de u. Déterminer le polynôme minimal et le polynôme caractéristique de u_v, et redémontrer ainsi le théorème de Cayley-Hamilton pour u.
Indication : montrer que, étant donné $P \in \Bbbk[X]$, $P(u_v) = \mathbf{0}_{\mathsf{L}(E_{u,v})}$ si et seulement si $P(u)(v) = \mathbf{0}_E$, et calculer la matrice de u_v dans la base donnée par $(v, u(v), \dots, u^{d-1}(v))$.

(e) Montrer que si $P \in \Bbbk[X]$, alors

$$P(u)(E_{u,v}) = E_{u,P(u)(v)} \text{ et } \mu_{u,v} = \mathsf{PGCD}(P, \mu_{u,v}).\mu_{u,P(u)(v)}.$$

(f) Déterminer $E_{u,v}$ et $\mu_{u,v}$ si

(i) $v = \mathbf{0}_E$;

(ii) v est un vecteur propre de u ;

(iii) il existe un entier $r > 1$ et des vecteurs propres $v_1, \dots, v_r$ de u associés à des valeurs propres distinctes tels que $v = v_1 + \cdots + v_r$.

(g) Montrer que si $(e_1, \dots, e_n)$ est une base de E, $I_{u,\Bbbk}$ est l'intersection des I_{u,e_k} et $\mu_{u,\Bbbk}$ est le PPCM des μ_{u,e_k}.

(h) Soit $\mu_{u,\Bbbk} = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition en facteurs irréductibles de $\mu_{u,\Bbbk}$, *i.e.* les polynômes P_k sont irréductibles et unitaires, P_i et P_j sont premiers entre eux pour $i \neq j$, et $\alpha_k \in \mathbb{N}^*$.

(i) Construire des vecteurs $v_1, \dots, v_r \in E$ tels que $\mu_{u,v_k} = P_k^{\alpha_k}$ pour tout k.

(ii) Montrer que les sous-espaces E_{u,v_k} sont en somme directe.
Indication : utiliser les noyaux $\mathsf{Ker}(P_k^{\alpha_k}(u))$.

(iii) Soit $v = v_1 + \cdots + v_r$. À l'aide de la question précédente, montrer que $\mu_{u,v} = \mu_{u,\Bbbk}$. Retrouver ainsi que le $\deg(\mu_{u,\Bbbk}) \leq n$ sans utiliser le théorème de Cayley-Hamilton.

(i) On dit que u est **cyclique** s'il existe $v \in E$ tel que $E_{u,v} = E$. Montrer que u est cyclique si et seulement si $\mu_{u,\Bbbk} = \chi_u$.

(j) Montrer que si u est cyclique et si F est un sous-espace vectoriel stable par u, alors l'endomorphisme induit $u_F = u|_F : F \to F$ est cyclique.
Indication : fixer un vecteur $v \in E$ tel que $E_{u,v} = E$ et montrer que l'ensemble $I = \{P \in \Bbbk[X] : P(u)(v) \in F\}$ est un idéal de $\Bbbk[X]$.

Solution.

(a) On voit bien que, étant donné $P \in \Bbbk[X]$, $u(P(u)(v)) = \tilde{P}(u)(v)$, où $\tilde{P}(X) = XP(X)$, ce qui nous dit que $u(w) \in E_{u,v}$ pour tout $w \in E_{u,v}$, comme on voulait démontrer.

(b) C'est clair que $I_{u,v}$ est un sous-espace vectoriel de $\Bbbk[X]$, vu que $\mathsf{ev}_{u,v} : \Bbbk[X] \to E$ est une application linéaire. En plus, comme $(QP)(u)(v) = Q(u)(P(u)(v))$ pour tous $P, Q \in \Bbbk[X]$, on voit bien que si $P \in I_{u,v}$, alors

$$(QP)(u)(v) = Q(u)(P(u)(v)) = Q(u)(\mathbf{0}_E) = \mathbf{0}_E,$$

ce qui implique que $QP \in I_{u,v}$. Le premier théorème d'isomorphisme d'espaces vectoriels nous dit alors que $\mathsf{ev}_{u,v} : \Bbbk[X] \to E$ induit une application linéaire injective $\bar{\mathsf{ev}}_{u,v} : \Bbbk[X]/I_{u,v} \to E$. Comme E est de dimension finie, $\Bbbk[X]/I_{u,v}$ est aussi de dimension finie, ce qui implique *a fortiori* que $I_{u,v} \neq \{0\}$, vu que $\Bbbk[X]$ est de dimension infinie.

(c) On remarque d'abord que l'image de l'application linéaire $\mathsf{ev}_{u,v} : \Bbbk[X] \to E$ est par définition $E_{u,v}$. À partir du premier théorème d'isomorphisme, on voit bien que l'application linéaire $\mathsf{ev}_{u,v} : \Bbbk[X] \to E$ induit une application linéaire injective $\overline{\mathsf{ev}}_{u,v} : \Bbbk[X]/(\mu_{u,v}) \to E$ avec la même image $E_{u,v}$ que $\mathsf{ev}_{u,v}$. D'après l'exercice 5 de la fiche 6, l'application linéaire $\iota : \Bbbk[X]_{\leq d-1} \to \Bbbk[X]/(\mu_{u,v})$ obtenue à partir de faire la composition de l'inclusion $\Bbbk[X]_{\leq d-1} \to \Bbbk[X]$ et la projection canonique $\Bbbk[X] \to \Bbbk[X]/(\mu_{u,v})$ est un isomorphisme linéaire, ce qui nous dit que $(\iota(1), \iota(X), \iota, \iota(X^{d-1}))$ est une base de $\Bbbk[X]/(\mu_{u,v})$. En conséquence,

$$\Big(\overline{\mathsf{ev}}_{u,v}\big(\iota(1)\big), \overline{\mathsf{ev}}_{u,v}\big(\iota(X)\big), \dots, \overline{\mathsf{ev}}_{u,v}\big(\iota(X^{d-1})\big)\Big) = \big(v, u(v), \dots, u^{d-1}(v)\big)$$

est une base $E_{u,v}$. On en déduit que $\mathsf{dim}(E_{u,v}) = d = \mathsf{deg}(\mu_{u,v})$.

(d) On montre d'abord que, étant donné $P \in \Bbbk[X]$, $P(u_v) = \mathbf{0}_{\mathsf{L}(E_{u,v})}$ si et seulement si $P(u)(v) = \mathbf{0}_E$. En effet, si $P(u_v) = \mathbf{0}_{\mathsf{L}(E_{u,v})}$, alors $P(u)(v) = P(u_v)(v) = \mathbf{0}_E$, et, réciproquement, si $P(u)(v) = \mathbf{0}_E$, alors

$$\begin{aligned} P(u_v)\big(Q(u)(v)\big) &= P(u)\big(Q(u)(v)\big) = (PQ)(u)(v) = (QP)(u)(v) = Q(u)\big(P(u)(v)\big) \\ &= Q(u)(\mathbf{0}_E) = \mathbf{0}_E, \end{aligned}$$

pour tout $Q \in \Bbbk[X]$, ce qui implique que $P(u_v) = \mathbf{0}_{\mathsf{L}(E_{u,v})}$. Cela nous dit que $P(u_v) = \mathbf{0}_{\mathsf{L}(E_{u,v})}$ si et seulement si $P \in I_{u,v}$, *i.e.* $P \in I_{u_v,\Bbbk}$ si et seulement si $P \in I_{u,v}$. En conséquence, $I_{u,v} = I_{u_v,\Bbbk}$, ce qui implique que $\mu_{u_v} = \mu_{u,v}$.

Par ailleurs, on suppose que $\mu_{v,u} = X^d + \sum_{i=0}^{d-1} a_i X^i \in \Bbbk[X]$. On voit bien que la matrice de u_v dans la base donnée par $(v, u(v), \dots, u^{d-1}(v))$ est

$$A_v = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{d-1} \end{pmatrix},$$

car $u(u^i(v)) = u^{i+1}(v)$ pour $i \in [\![0, d-2]\!]$ et $u(u^{d-1}(v)) = u^d(v) = -\sum_{i=0}^{d-1} a_i u^i(v)$. Un argument par récurrence sur d nous dit que

$$\mathsf{det}(\lambda\,\mathsf{I}_d - A_v) = \begin{pmatrix} \lambda & 0 & \dots & 0 & a_0 \\ -1 & \lambda & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & \lambda + a_{d-1} \end{pmatrix} = \lambda^d + \sum_{i=0}^{d-1} a_i \lambda^i,$$

ce qui nous dit que $\chi_{u_v} = \mu_{u,v}$.

Pour démontrer le théorème de Cayley-Hamilton pour u, *i.e.* $\chi_u(u) = \mathbf{0}_{\mathsf{L}(E)}$, on va d'abord montrer que χ_{u_v} divise χ_u dans $\Bbbk[X]$ pour tout $v \in E$. On sait que l'ensemble libre $(v, u(v), \dots, u^{d-1}(v))$ de E est partie d'une base $\mathscr{B} = (v, u(v), \dots, u^{d-1}(v), w_1, \dots, w_{n-d})$ de E. La matrice de u dans la base $\mathscr{B}$ est

$$A = \left(\begin{array}{c:c} A_v & B \\ \hdashline \mathbf{0} & C \end{array}\right),$$

où $\mathbf{0}$ est la matrice nulle de $\mathsf{M}_{(n-d)\times d}(\Bbbk)$, $B \in \mathsf{M}_{d\times(n-d)}(\Bbbk)$ et $C \in \mathsf{M}_{(n-d)\times(n-d)}(\Bbbk)$. Cela implique que

$$\mathsf{det}(\lambda\,\mathsf{I}_n - A) = \mathsf{det}\left(\begin{array}{c:c} \lambda\,\mathsf{I}_d - A_v & B \\ \hdashline \mathbf{0} & \lambda\,\mathsf{I}_{n-d} - C \end{array}\right) = \mathsf{det}(\lambda\,\mathsf{I}_d - A_v).\,\mathsf{det}(\lambda\,\mathsf{I}_{n-d} - C),$$

i.e. χ_{u_v} divise χ_u dans $\Bbbk[X]$.

Finalement, comme, étant donné $v \in E$ il existe $P_v \in \Bbbk[X]$ tel que $\chi_u = P_v \chi_{u_v}$, on a que

$$\chi_u(u)(v) = P_v(u)(\chi_{u_v}(u)(v)) = P_v(u)(\mathbf{0}_E) = \mathbf{0}_E,$$

i.e. $\chi_u(u) = \mathbf{0}_{\mathsf{L}(E)}$.

(e) On voit bien que

$$P(u)\big(Q(u)(v)\big) = (PQ)(u)(v) = (QP)(u)(v) = Q(u)\big(P(u)(v)\big) \tag{9}$$

pour tout $Q \in \Bbbk[X]$, ce qui implique que $P(u)(E_{u,v}) = E_{u,P(u)(v)}$. En outre, (9) nous dit aussi que, étant donné $Q \in \Bbbk[X]$, $Q \in I_{u,P(u)(v)}$ si et seulement si $QP \in I_{u,v}$, *i.e.* étant donné $Q \in \Bbbk[X]$, $\mu_{u,P(u)(v)}$ divise Q si et seulement si $\mu_{u,v}$ divise $Q.P$. Cette dernière condition est équivalente à que $\mu_{u,v}$ divise $Q.\,\mathsf{PGCD}(P,\mu_{u,v})$. En effet, on affirme que $R \in \Bbbk[X]$ divise $Q.P$ dans $\Bbbk[X]$ si et seulement si $R \in \Bbbk[X]$ divise $Q.\,\mathsf{PGCD}(P,R)$ dans $\Bbbk[X]$. Pour le montrer, on note que $P = \mathsf{PGCD}(P,R).\hat{P}$ avec $\hat{P}$ et R premiers entre eux, ce qui nous dit que R divise $Q.P = Q.\,\mathsf{PGCD}(P,R).\hat{P}$ si et seulement si R divise $Q.\,\mathsf{PGCD}(P,R)$, d'après le lemme d'Euclide pour $\Bbbk[X]$. En conséquence, étant donné $Q \in \Bbbk[X]$, $\mu_{u,P(u)(v)}$ divise Q si et seulement si $\mu_{u,v}$ divise $Q.\,\mathsf{PGCD}(P,\mu_{u,v})$. En choisissant $Q = \mu_{u,v}/\,\mathsf{PGCD}(P,\mu_{u,v})$, on conclut que $\mu_{u,P(u)(v)}$ divise $\mu_{u,v}/\,\mathsf{PGCD}(P,\mu_{u,v})$, *i.e.* $\mathsf{PGCD}(P,\mu_{u,v}).\mu_{u,P(u)(v)}$ divise $\mu_{u,v}$. En outre, en choisissant $Q = \mu_{u,P(u)(v)}$, on voit que $\mu_{u,v}$ divise $\mathsf{PGCD}(P,\mu_{u,v}).\mu_{u,P(u)(v)}$, ce qui implique $\mu_{u,v} = \mathsf{PGCD}(P,\mu_{u,v}).\mu_{u,P(u)(v)}$, vu qu'il s'agit de polynômes unitaires.

(f) On voit bien que $E_{u,\mathbf{0}_E} = \{\mathbf{0}_E\}$ et $\mu_{u,\mathbf{0}_E} = 1$. En outre, c'est clair que si v est un vecteur propre avec valeur propre $\lambda \in \Bbbk$, alors $E_{u,v} = \mathsf{Vect}_{\Bbbk}\langle\{v\}\rangle$ et $\mu_{u,v} = X - \lambda$. Finalement, on suppose qu'il existe un entier $r > 1$ et des vecteurs propres $v_1, \dots, v_r$ de u associés à des valeurs propres $\lambda_1, \dots, \lambda_r$ distinctes. Soit $v = v_1 + \cdots + v_r$. On affirme d'abord que $E_{u,v} = \mathsf{Vect}_{\Bbbk}\langle\{v_1, \dots, v_r\}\rangle$. En effet, l'inclusion $E_{u,v} \subseteq \mathsf{Vect}_{\Bbbk}\langle\{v_1, \dots, v_r\}\rangle$ est immédiate, vu que

$$P(u)(v) = P(u)\Big(\sum_{i=1}^{r} v_i\Big) = \sum_{i=1}^{r} P(u)(v_i) = \sum_{i=1}^{r} P(\lambda_i)v_i \in \mathsf{Vect}_{\Bbbk}\langle\{v_1, \dots, v_r\}\rangle \tag{10}$$

pour tout $P \in \Bbbk[X]$. Pour montrer l'inclusion $\mathsf{Vect}_{\Bbbk}\langle\{v_1, \dots, v_r\}\rangle \subseteq E_{u,v}$ il suffit de montrer que $v_i \in E_{u,v}$ pour tout $i \in [\![1,r]\!]$, *i.e.* il existe $P_i \in \Bbbk[X]$ tel que $P_i(u)(v) = v_i$ pour tout $i \in [\![1,r]\!]$. On définit pour cela

$$P_i = \prod_{\substack{j \in [\![1,r]\!],\\ j \neq i}} \frac{X - \lambda_j}{\lambda_i - \lambda_j} \in \Bbbk[X].$$

Alors, le calcul dans (10) nous dit que On voit bien que $P_i(u)(v_j) = \mathbf{0}_E$ pour tous $i, j \in [\![1,r]\!]$ avec $i \neq j$, ce qui nous dit que

$$P_i(u)(v) = P_i(u)\Big(\sum_{i=1}^{r} v_i\Big) = \sum_{j=1}^{r} P_i(u)(v_j) = \sum_{j=1}^{r} P_i(\lambda_j)v_j = P_i(\lambda_i)v_i = v_i,$$

où l'on a utilisé que $P_i(\lambda_j) = 0$ pour tous $i, j \in [\![1,r]\!]$ avec $i \neq j$, et $P_i(\lambda_i) = 1$ pour tout $i \in [\![1,r]\!]$. On affirme finalement que $\mu_{u,v} = \prod_{i=1}^{r}(X - \lambda_i)$. en effet, c'est clair que le polynôme unitaire $\prod_{i=1}^{r}(X - \lambda_i)$ satisfait

$$\prod_{i=1}^{r}(u - \lambda_i)(v) = \sum_{j=1}^{r}\prod_{i=1}^{r}(u - \lambda_i)(v_j) = \mathbf{0}_E$$

et $\mathsf{deg}(\prod_{i=1}^{r}(X - \lambda_i)) = r = \mathsf{dim}(E_{u,v})$, ce qui nous dit que $\mu_{u,v} = \prod_{i=1}^{r}(X - \lambda_i)$.

(*g*) On voit bien que $P \in \cap_{i=1}^{n} I_{u,e_i}$ si et seulement si $P(u)(e_i) = \mathbf{0}_E$ pour tout $i \in [\![1,n]\!]$, ce qui équivaut à $P(u)(v) = \mathbf{0}_E$ pour tout $v \in E$, *i.e.* $P(u) = \mathbf{0}_{\mathsf{L}(E)}$, ce qui équivaut à $P \in I_{u,\Bbbk}$. En conséquence, $I_{u,\Bbbk} = \cap_{i=1}^{n} I_{u,e_i}$. Cela nous dit que, étant donné $P \in \Bbbk[X]$, $\mu_{u,\Bbbk}|P$ si et seulement si $\mu_{u,e_i}|P$ pour tout $i \in [\![1,n]\!]$. En particulier, $\mu_{u,\Bbbk}$ divise $\mathsf{PPCM}(\mu_{u,e_1},\dots,\mu_{u,e_n})$, et $\mu_{u,e_i}|\mu_{u,\Bbbk}$ pour tout $i \in [\![1,n]\!]$, ce qui implique que $\mathsf{PPCM}(\mu_{u,e_1},\dots,\mu_{u,e_n})$ divise $\mu_{u,\Bbbk}$. En conséquence, $\mu_{u,\Bbbk} = \mathsf{PPCM}(\mu_{u,e_1},\dots,\mu_{u,e_n})$, vu que les deux polynômes sont unitaires.

(*h*) (i) Soient $Q_i = \mu_{u,\Bbbk}/P_i \in \Bbbk[X]$ et $R_i = \mu_{u,\Bbbk}/P_i^{\alpha_i} \in \Bbbk[X]$ pour tout $i \in [\![1,r]\!]$. Comme $\mathsf{deg}(Q_i) < \mathsf{deg}(\mu_{u,\Bbbk})$, $Q_i(u) \neq \mathbf{0}_{\mathsf{L}(E)}$, ce qui nous dit qu'il existe $w_i \in E$ tel que $Q_i(u)(w_i) \neq \mathbf{0}_E$. Soit $v_i = R_i(u)(w_i)$. Or, comme $\mu_{u,\Bbbk} = P_i^{\alpha_i} R_i$, on a alors

$$P_i^{\alpha_i}(u)(v_i) = P_i^{\alpha_i}(u)(R_i(u)(w_i)) = \mu_{u,\Bbbk}(u)(w_i) = \mathbf{0}_E,$$

ce qui nous dit que $P_i^{\alpha_i} \in I_{u,v_i}$, ce qui implique que μ_{u,v_i} divise $P_i^{\alpha_i}$. Comme P_i est irréductible et unitaire, on conclut que $P_i^{\ell_i} = \mu_{u,v_i}$ avec $\ell_i \in [\![1,\alpha_i]\!]$. En outre, comme $P_i^{\alpha_i-1}(u)(v_i) = Q_i(u)(w_i) \neq \mathbf{0}_E$, on voit que $P_i^{\alpha_i-1} \notin I_{u,v_i}$, ce qui implique que $\ell_i = \alpha_i$. En conséquence, $P_i = \mu_{u,v_i}$.

(ii) On note d'abord que $E_{u,v_i} \subseteq \mathsf{Ker}(P_i^{\alpha_i}(u))$ pour tout $i \in [\![1,r]\!]$. En effet, si $x \in E_{u,v_i}$, alors $x = T(u)(v_i)$ avec $T \in \Bbbk[X]$, ce qui implique que

$$P_i^{\alpha_i}(u)(x) = P_i^{\alpha_i}(u)\big(T(u)(v_i)\big) = (P_i^{\alpha_i}T)(u)(v_i) = T(u)\big(P_i^{\alpha_i}(u)(v_i)\big) = T(u)(\mathbf{0}_E) = \mathbf{0}_E,$$

i.e. $E_{u,v_i} \subseteq \mathsf{Ker}(P_i^{\alpha_i}(u))$. Or l'exercice **11** nous dit que les sous espaces $\mathsf{Ker}(P_i^{\alpha_i}(u))$ pour $i \in [\![1,r]\!]$ sont en somme directe. En effet, la dernière identité de l'exercice **11** implique que $\mathsf{Ker}(R_i(u)) = \sum_{j\neq i} \mathsf{Ker}(P_j^{\alpha_j}(u))$, tandis que la première identité nous dit que

$$\{\mathbf{0}_E\} = \mathsf{Ker}(\mathsf{id}_E) = \mathsf{Ker}\left(P_i^{\alpha_i}(u)\right) \cap \mathsf{Ker}\left(R_i(u)\right) = \mathsf{Ker}\left(P_i^{\alpha_i}(u)\right) \cap \Big(\sum_{j\neq i} \mathsf{Ker}\left(P_j^{\alpha_j}(u)\right)\Big).$$

Finalement, l'exercice **11** nous dit aussi que

$$E = \mathsf{Ker}(\mathbf{0}_{\mathsf{E}}) = \mathsf{Ker}\left(\mu_{u,\Bbbk}(u)\right) = \sum_{i=1}^{r} \mathsf{Ker}\left(P_j^{\alpha_j}(u)\right) = \bigoplus_{i=1}^{r} \mathsf{Ker}\left(P_j^{\alpha_j}(u)\right) \tag{11}$$

(iii) On voit bien que $P(u)(v) = \mathbf{0}_E$ si et seulement si $P(u)(v_i) = \mathbf{0}_E$ pour tout $i \in [\![1,r]\!]$, vu que $P(u)(v_i) \in E_{u,v_i}$ pour tout $i \in [\![1,r]\!]$ et la famille de sous-espaces $\{E_{u,v_i} : i \in [\![1,r]\!]\}$ est libre. En conséquence, $\mu_{u,v}$ divise P si et seulement si $\mu_{u,v_i} = P_i^{\alpha_i}$ divise P pour tout $i \in [\![1,r]\!]$, ce qui équivaut à $\mu_{u,\Bbbk} = \prod_{i=1}^{r} P_i^{\alpha_i}$ divise P. En conséquence, $\mu_{u,v} = \mu_{u,\Bbbk}$, vu que les deux polynômes sont unitaires. Comme $\mathsf{deg}(P_i^{\alpha_i}) = \mathsf{dim}(E_{u,v_i}) \leq \mathsf{dim}(\mathsf{Ker}(P_i^{\alpha_i}(u)))$ pour tout $i \in [\![1,r]\!]$, (11) nous dit que

$$\mathsf{deg}(\mu_{u,\Bbbk}) = \sum_{i=1}^{r} \mathsf{deg}(P_i^{\alpha_i}) \leq \sum_{i=1}^{r} \mathsf{dim}\Big(\mathsf{Ker}\left(P_i^{\alpha_i}(u)\right)\Big) = n.$$

(*i*) On remarque d'abord que, vu que $\mu_{u,\Bbbk}|\chi_u$ et les polynômes sont unitaires, $\mu_{u,\Bbbk} = \chi_u$ si et seulement si $\mathsf{deg}(\mu_{u,\Bbbk}) = \mathsf{dim}(E) = n$. En outre, si $v \in E$, alors $\mu_{u,v}|\mu_{u,\Bbbk}$, vu que $\mu_{u,\Bbbk}(u)(v) = \mathbf{0}_E$, ce qui implique $\mathsf{deg}(\mu_{u,v}) \leq \mathsf{deg}(\mu_{u,\Bbbk})$. Si u est cyclique et $v \in E$ est tel que $E_{u,v} = E$, alors $\mathsf{deg}(\mu_{u,v}) = \mathsf{dim}(E_{u,v}) = \mathsf{dim}(E) = n \geq \mathsf{deg}(\mu_{u,\Bbbk})$, ce qui implique $n = \mathsf{deg}(\mu_{u,\Bbbk})$ et, en conséquence, $\mu_{u,\Bbbk} = \chi_u$. Réciproquement, si $\mathsf{deg}(\mu_{u,\Bbbk} = \chi_u$, soit $v \in E$ tel que $\mu_{u,v} = \mu_{u,\Bbbk}$, qui existe pour l'item précédent. Alors, $\mathsf{dim}(E_{u,v}) = \mathsf{deg}(\mu_{u,v}) = \mathsf{deg}(\mu_{u,\Bbbk}) = n$, ce qui implique que $E_{u,v} = E$, *i.e.* u est cyclique.

(j) Soit $v \in E$ tel que $E_{u,v} = E$. Alors, l'ensemble $I = \{P \in \Bbbk[X] : P(u)(v) \in F\}$ est un idéal de $\Bbbk[X]$. En effet, I est un sous-espace vectoriel de $\Bbbk[X]$ car $I = \mathrm{ev}_{u,v}^{-1}(F)$ est l'image réciproque d'un sous-espace vectoriel par une application linéaire. En outre, si $P \in \Bbbk[X]$ et $Q \in I$, alors $PQ \in I$, car $(PQ)(u)(v) = P(u)(Q(u)(v)) \in F$, vu que $Q(u)(v) \in F$ et F est stable par l'application u. Alors, il existe $P_0 \in \Bbbk[X]$ tel que $I = (P_0)$ est l'idéal engendré par P_0. Soit $w = P_0(v)$. Noter que $w \in F$, vu que $P_0 \in I$. En plus, si $w' \in F \subseteq E$, il existe $T \in \Bbbk[X]$ tel que $T(u)(v) = w'$. Par définition, $T \in I$, ce qui implique que $T = \hat{T} P_0$ avec $\hat{T} \in \Bbbk[X]$. En conséquence, $w' = T(u)(v) = \hat{T}(u)(P_0(u)(v)) = \hat{T}(u)(w)$, ce qui implique que $E_{u|_F,w} = E_{u,w} = F$, et $u|_F$ est cyclique.

13. Soient E un $\Bbbk$-espace vectoriel de dimension n et $u \in \mathsf{L}(E)$ un endomorphisme nilpotent d'indice d, *i.e.* d est le plus petit entier $k \geq 1$ tel que $u^k = \mathbf{0}_{\mathsf{L}(E)}$.

(a) Montrer qu'il existe $a \in E$ et $\varphi \in E^*$ tels que $\varphi(u^{d-1}(a)) \neq 0$.

(b) Montrer que $\{a, u(a), \dots, u^{d-1}(a)\}$ et $\{\varphi, \varphi \circ u, \dots, \varphi \circ u^{d-1}\}$ sont libres.

(c) On note F et Φ le sous-espace vectoriel engendré par ces familles. Montrer que F et $\Phi_\perp$ sont stables par u et supplémentaires.

(d) En déduire par récurrence sur la dimension de E qu'il existe une base de E dans laquelle la matrice de u est diagonale par blocs avec des blocs de Jordan nilpotents sur la diagonale, *i.e.* de la forme

$$J_{d'} = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \in \mathsf{M}_{d'}(\Bbbk),$$

avec $0 < d' \leq d$.

Solution.

(a) Comme $u^{d-1} \neq \mathbf{0}_{\mathsf{L}(E)}$, il existe $a \in E$ tel que $u^{d-1}(a) \neq \mathbf{0}_E$. En conséquence, il existe $\varphi \in E^*$ tel que $\varphi(u^{d-1}(a)) \neq 0$, comme on voulait démontrer.

(b) On définit $F^k = \mathsf{Ker}(u^{d-k})$ pour $k \in [\![0, d]\!]$. C'est clair que $F^0 = E$, $F^d = \{\mathbf{0}_E\}$ et $F^{k+1} \subseteq F^k$ pour tout $k \in [\![0, d-1]\!]$. En outre, par définition $a \in F^0 \setminus F^1$. De façon plus générale, in argument par récurrence sur k nous dit que $u^k(a) \in F^k \setminus F^{k+1}$ pour tout $k \in [\![0, d-1]\!]$. En particulier, $F^{k+1} \subsetneq F^k$ pour tout $k \in [\![0, d-1]\!]$. On notera $\pi_k : E \to E/F^k$ la projection canonique, pour $k \in [\![0, d]\!]$. Or, on considère $v = \sum_{k=0}^{d-1} c_k u^k(a) = \mathbf{0}_E$. On va montrer que cela implique que $c_0 = \dots = c_{d-1} = 0$. Soit $k_0 = \min\{k \in [\![0, d-1]\!] : c_k \neq 0\}$. Alors, comme $u^k(a) \in F^{k_0+1}$ si $k \geq k_0 + 1$,

$$\mathbf{0}_{E/F^{k_0+1}} = \pi_{k_0+1}(\mathbf{0}_E) = \pi_{k_0+1}(v) = \sum_{k=k_0}^{d-1} c_k \pi_{k_0+1}\big(u^k(a)\big) = \underbrace{c_{k_0}}_{\neq 0} \underbrace{\pi_{k_0+1}\big(u^{k_0}(a)\big)}_{\neq \mathbf{0}_{E/F^{k_0+1}}},$$

ce qui est absurde. En conséquence, $\{a, u(a), \dots, u^{d-1}(a)\}$ est un ensemble libre.

Pour montrer que $\{\varphi, \varphi \circ u, \dots, \varphi \circ u^{d-1}\}$ est un ensemble libre il suffit d'appliquer le résultat précédent avec ${}^t u$ au lieu de u et φ au lieu de a, vu que $\varphi \circ u^k = ({}^t u)^k(\varphi)$, $({}^t u)^d = \mathbf{0}_{\mathsf{L}(E^*)}$ et $({}^t u)^{d-1}(\varphi) \neq \mathbf{0}_{E^*}$.

(*c*) C'est clair que $u(F) \subseteq F$, vu que $u(\sum_{k=0}^{d-1} c_k u^k(a)) = \sum_{k=0}^{d-2} c_k u^{k+1}(a)$, pour $c_k \in \Bbbk$ pour tout $k \in [\![0, d-1]\!]$. Le même argument avec ${}^t u$ au lieu de u et φ au lieu de a nous dit que ${}^t u(\Phi) \subseteq \Phi$. D'après l'exercice **5**, (b), nous dit que $u(\Phi_\perp) \subseteq \Phi_\perp$. D'après les commentaires dans le dernier item de l'exercice **4**, on sait que $\dim(\Phi_\perp) = \dim(E) - \dim(\Phi) = \dim(E) - \dim(F)$. En outre, on voit bien que $F \cap \Phi_\perp = \{\mathbf{0}_E\}$, car si $v = \sum_{k=0}^{d-1} c_k u^k(a) \neq \mathbf{0}_E$, où $c_k \in \Bbbk$ pour tout $k \in [\![0, d-1]\!]$, et $k_0 = \max\{k \in [\![0, d-1]\!] : c_k \neq 0\}$, alors $(\varphi \circ u^{d-k_0-1})(v) = c_{k_0}\varphi(u^{d-1}(a)) \neq 0$, ce qui nous dit que $v \notin \Phi_\perp$. Comme $F \cap \Phi_\perp = \{\mathbf{0}_E\}$ et $\dim(\Phi_\perp) + \dim(F) = \dim(E)$, on conclut que $F \oplus \Phi_\perp = E$.

(*d*) On suppose qu'il existe des sous-espaces indépendants $F_1, \dots, F_\ell \subseteq E$ tels que $u(F_i) \subseteq F_i$ et tels que F_i possède une base de la forme $\{a_i, u(a_i), \dots, u^{d_i-1}(a_i)\}$ où $0 < d_i \leq d$ pour tout $i \in [\![1, \ell]\!]$. Pour tout $i \in [\![1, \ell]\!]$ on choisit $\varphi_i \in E^*$ tel que $\varphi_i(u^{d_i-1}(a_i)) \neq 0$. On considère alors les sous-espaces $\Phi_1, \dots, \Phi_\ell \subseteq E^*$ avec Φ_i engendré par la base de la forme $\{\varphi_i, \varphi_i \circ u, \dots, \varphi_i \circ u^{d_i-1}\}$ pour tout $i \in [\![1, \ell]\!]$. On pose $F = F_1 \oplus \cdots \oplus F_\ell$ et $G = (\Phi_1)_\perp \cap \cdots \cap (\Phi_\ell)_\perp$. Alors, on voit bien que $F \oplus G = E$. Le cas $\ell = 1$ a été démontré dans l'item précédent. On montrera que si $F \neq E$, alors on peut construire $F_{\ell+1}$ de sorte que $F_1, \dots, F_{\ell+1} \subseteq E$ satisfasse les propriétés précédentes. En effet, on note que $u(G) \subseteq G$, vu que $u((\Phi_i)_\perp) \subseteq (\Phi_i)_\perp$ pour tout $i \in [\![1, \ell]\!]$. En outre, comme $u^d = 0$, il existe $0 < d' \leq d$ tel que $(u|_G)^{d'} = \mathbf{0}_{\mathsf{L}(G)}$ et $(u|_G)^{d'-1} = \mathbf{0}_{\mathsf{L}(G)}$. En appliquant l'item précédent à $u|_G : G \to G$ on construit $F_{\ell'+1} \subseteq G$ avec une base de la forme une base de la forme $\{a_{\ell'+1}, u(a_{\ell'+1}), \dots, u^{d_{\ell'+1}-1}(a_i)\}$ où $0 < d' = d_{\ell'+1} \leq d$. Par récurrence, on conclut qu'il existe une décomposition $F_1 \oplus \cdots \oplus F_\ell = E$ tels que $u(F_i) \subseteq F_i$ et tels que F_i possède une base de la forme $\{a_i, u(a_i), \dots, u^{d_i-1}(a_i)\}$ où $0 < d_i \leq d$ pour tout $i \in [\![1, \ell]\!]$. On note finalement, que la représentation matricielle de $u|_{F_i} : F_i \to F_i$ dans la base $\{a_i, u(a_i), \dots, u^{d_i-1}(a_i)\}$ est de la forme J_{d_i} pour tout $i \in [\![1, \ell]\!]$.

14. Soit E un $\Bbbk$-espace vectoriel de dimension finie n et soit $u \in \mathsf{L}(E)$. On suppose qu'on dispose d'un polynôme P annulateur de u, unitaire et scindé qu'on décompose en facteurs irréductibles de la forme

$$P = (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}.$$

Pour tout $i \in [\![1, r]\!]$, on note $E_i = \mathsf{Ker}(u - \alpha_i \,\mathsf{id}_E)^{m_i}$.

(*a*) Montrer que $E = E_1 \oplus \cdots \oplus E_r$.
Indication : utiliser le théorème de décomposition des noyaux.

(*b*) Soient $p_1, \dots, p_r : E \to E$ les projections associées à la décomposition d'espaces vectoriels $E = E_1 \oplus \cdots \oplus E_r$. Montrer que chaque E_i est stable par u, et en déduire que u commute avec chaque projection p_i.

(*c*) On note $u|_{E_i} : E_i \to E_i$ l'endomorphisme induit par u sur E_i. Montrer que $u|_{E_i} - \alpha_i \,\mathsf{id}_{E_i}$ est nilpotent. En utilisant l'exercice précédent, en déduire que dans une base convenable u admet une matrice diagonale par blocs, avec des blocs de Jordan sur la diagonale (*i.e.* de la forme $J_{d'} + \alpha_i I_{d'}$, avec $0 < d' \leq m_i$).

(*d*) Soient $d = \alpha_1 p_1 + \cdots + \alpha_r p_r$ et $v = u - d$. Montrer que d est diagonalisable, v est nilpotent, d et v commutent.

Solution.

(a) On rappelle que, si $P_1, \dots, P_r \in \Bbbk[X]$ sont polynômes premiers entre eux, alors il existe $Q_1, \dots, Q_r \in \Bbbk[X]$ tels que $\sum_{i=1}^r Q_i P_i = 1$. Soit $P = P_1 \dots P_r$ et $u \in \mathsf{L}(E)$. On note aussi que les polynômes $P/P_1, \dots, P/P_r \in \Bbbk[X]$ sont aussi premiers entre eux, ce qui nous dit qu'il existe $S_1, \dots, S_r \in \Bbbk[X]$ tels que $\sum_{i=1}^r S_i P/P_i = 1$. Alors, le théorème de décomposition des noyaux nous dit que

$$\mathsf{Ker}\big(P(u)\big) = \mathsf{Ker}\big(P_1(u)\big) \oplus \dots \oplus \mathsf{Ker}\big(P_r u)\big). \tag{12}$$

En effet, $P(u) = P_1(u) \dots P_r(u)$ nous dit que $\mathsf{Ker}(P_i(u)) \subseteq \mathsf{Ker}(P(u))$ pour tout $i \in [\![1, r]\!]$, ce qui implique que

$$\mathsf{Ker}\big(P(u)\big) \supseteq \mathsf{Ker}\big(P_1(u)\big) + \dots + \mathsf{Ker}\big(P_r u)\big).$$

En outre, $\sum_{i=1}^r S_i P/P_i = 1$ nous dit que $\sum_{i=1}^r S_i(u) \circ (P/P_i)(u) = \mathsf{id}_E$, ce qui implique que, si $v \in \mathsf{Ker}(P(u))$, alors $(S_i(u) \circ (P/P_i)(u))(v) \in \mathsf{Ker}(P_i(u))$ pour tout $i \in [\![1, r]\!]$. En conséquence, comme $v = \sum_{i=1}^r (S_i(u) \circ (P/P_i)(u))(v)$, on trouve que

$$\mathsf{Ker}\big(P(u)\big) \subseteq \mathsf{Ker}\big(P_1(u)\big) + \dots + \mathsf{Ker}\big(P_r u)\big).$$

On note finalement que la dernière sommes est directe. En effet, étant donne $\mathbf{0}_E = \sum_{i=1}^r v_i$ avec $v_i \in \mathsf{Ker}(P_i(u))$ pour $i \in [\![1, r]\!]$, il faut montrer que $\mathbf{0}_E = v_i$ pour tout $i \in [\![1, r]\!]$. Pour le démontrer, on note que

$$v_i = -\sum_{j \neq i} v_j \in \mathsf{Ker}\big(P_i(u)\big) \cap \bigg(\sum_{j \neq i} \mathsf{Ker}\big(P_j(u)\big)\bigg). \tag{13}$$

Comme les polynômes P_i et P/P_i sont premiers entre eux, il existe $R_i, T_i \in \Bbbk[X]$ tels que $R_i P_i + T_i P/P_i = 1$, ce qui nous dit avec (13) que

$$\mathbf{0}_E = \big(R_i(u) \circ P_i(u)\big)(v_i) + \big(T_i(u) \circ (P/P_i)(u)\big)(v_i) = v_i$$

pour tout $i \in [\![1, r]\!]$, comme on voulait démontrer.

Comme les polynômes $(X - \alpha_1)^{m_1}, \dots (X - \alpha_r)^{m_r}$ sont premiers entre eux, (12) nous dit que

$$E_1 \oplus \dots \oplus E_r = \mathsf{Ker}\big((u - \alpha_1 \, \mathsf{id}_E)^{m_1}\big) \oplus \dots \oplus \mathsf{Ker}\big((u - \alpha_r \, \mathsf{id}_E)^{m_r}\big) = \mathsf{Ker}\big(P(u)\big) = E.$$

(b) Comme $u \circ (u - \alpha_i \, \mathsf{id}_E)^{m_i} = (u - \alpha_i \, \mathsf{id}_E)^{m_i} \circ u$, on conclut que $u(E_i) \subseteq E_i$, pour tout $i \in [\![1, r]\!]$. En conséquence, si l'on écrit $v = \sum_{i=1}^r p_i(v)$ pour $v \in E$, on voit bien que $\sum_{i=1}^r p_i(u(v)) = u(v) = \sum_{i=1}^r u(p_i(v))$, ce qui implique $p_i \circ u = u \circ p_i$, pour tout $i \in [\![1, r]\!]$, vu que $E = E_1 \oplus \dots \oplus E_r$.

(c) On voit bien que, par définition de E_i, $(u_{E_i} - \alpha_i \, \mathsf{id}_{E_i})^{m_i} = \mathbf{0}_{\mathsf{L}(E_i)}$, *i.e.* $u|_{E_i} - \alpha_i \, \mathsf{id}_{E_i}$ est nilpotent. D'après l'exercice **13**, il existe une base $\mathscr{B}_i$ de E_i tel que la représentation matricielle de $u|_{E_i} - \alpha_i \, \mathsf{id}_{E_i}$ dans cette base est une matrice diagonale par blocs, avec des blocs de la forme $\{J_{m_{i,p}} : p \in \mathscr{I}_i\}$, où $\mathscr{I}_i$ est un ensemble fini d'indices, et $0 < m_{i,p} \leq m_i$. En conséquence, la représentation matricielle de u dans la base $\mathscr{B} = \mathscr{B}_1 \cup \dots \cup \mathscr{B}_r$ est une matrice diagonale par blocs, avec des blocs de Jordan sur la diagonale de la forme $\{J_{m_{i,p}} + \alpha_i I_{m_{i,p}} : i \in [\![1, r]\!], p \in \mathscr{I}_i\}$.

(d) Soient $d = \alpha_1 p_1 + \dots + \alpha_r p_r$ et $v = u - d$. C'est clair que la représentation matricielle de d dans la base $\mathscr{B}$ est la matrice diagonale formée des blocs $\{\alpha_i I_{m_{i,p}} : i \in [\![1, r]\!], p \in \mathscr{I}_i\}$, tandis que la représentation matricielle de v dans la base $\mathscr{B}$ est la matrice diagonale par blocs formée des blocs $\{J_{m_{i,p}} : i \in [\![1, r]\!], p \in \mathscr{I}_i\}$. En conséquence, d est diagonalisable et v est nilpotent. En plus, comme les blocs indexés par $i \in [\![1, r]\!]$ et $p \in \mathscr{I}_i$ de d et v commutent, vu que $J_{m_{i,p}}$ et $I_{m_{i,p}}$ commutent, on conclut que d et v commutent.

15. Montrer que tout endomorphisme d'un espace vectoriel de dimension $n \in \mathbb{N}^*$ admettant un polynôme annulateur scindé est trigonalisable.

Solution. Il s'agit d'une conséquence immédiate de l'exercice **14**.

16. Soient E un $\Bbbk$-espace vectoriel de dimension finie, $u \in \mathsf{L}(E)$ et χ_u le polynôme caractéristique de u. On se propose de montrer que si u est trigonalisable alors χ_u est scindé et $\chi_u(u) = \mathbf{0}_{\mathsf{L}(E)}$. Pour cela, on prend une base $\mathscr{B} = (e_1, \dots, e_n)$ de E dans laquelle la matrice de u est triangulaire supérieure et on note $A = (a_{i,j})_{1 \leq i,j \leq n}$ la matrice de u dans $\mathscr{B}$. Pour tout $k \in [\![0, n]\!]$, on note $F_k = \langle \{e_1, \dots, e_k\} \rangle$.

(a) Que vaut χ_u ?

(b) Montrer que pour tout $k \in [\![1, n]\!]$, $(u - a_{k,k}\,\mathsf{id}_E)(F_k) \subseteq F_{k-1}$.

(c) Conclure.

Solution.

(a) On voit bien que $\chi_u(X) = \det(u - X\,\mathsf{id}_E) = \prod_{i=1}^{n}(X - a_{i,i})$, vu que A est triangulaire supérieure, ce qui nous dit que χ_u est scindé.

(b) Comme $[u]_{\mathscr{B}\mathscr{B}} = A$, alors

$$u(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$$

pour tout $j \in [\![1, n]\!]$. Comme A est triangulaire supérieure, *i.e.* $A_{i,j} = 0$ si $i > j$, alors $u(e_j) \in F_j$ pour tout $j \in [\![1, n]\!]$. En conséquence, $(u - a_{k,k}\,\mathsf{id}_E)(e_j) = u(e_j) - a_{k,k}e_j \in F_{k-1}$ pour tout $j \in [\![1, k-1]\!]$ et $(u - a_{k,k}\,\mathsf{id}_E)(e_k) = u(e_k) - a_{k,k}e_k = \sum_{j=1}^{k-1} a_{k,j-1}u_j \in F_{k-1}$, ce qui implique que $(u - a_{k,k}\,\mathsf{id}_E)(F_k) \subseteq F_{k-1}$ $k \in [\![1, n]\!]$.

(c) Un argument immédiat par récurrence sur j (et k fixe) nous dit que

$$\prod_{k=j+1}^{k} (u - a_{j,j}\,\mathsf{id}_E)(F_k) \subseteq F_j \tag{14}$$

pour tous $j, k \in [\![0, n]\!]$ avec $j < k$. En effet, le cas $j = k - 1$ est précisément l'item précédent, et si

$$\prod_{i=j+2}^{k} (u - a_{i,i}\,\mathsf{id}_E)(F_k) \subseteq F_{j+1}$$

pour $j < k - 1$, alors

$$\prod_{i=j+1}^{k} (u - a_{i,i}\,\mathsf{id}_E)(F_k) \subseteq (u - a_{j+1,j+1}\,\mathsf{id}_E)(F_{j+1}) \subseteq F_j,$$

où l'on a utilisé l'item précédent. Finalement, (14) pour $j = 0$ implique que $\chi_u(u) = \mathbf{0}_{\mathsf{L}(E)}$, comme on voulait démontrer.

Calcul de formes de Jordan

17. Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ l'endomorphisme linéaire dont la matrice dans la base canonique (e_1, e_2, e_3) est

$$M = \begin{pmatrix} 3 & 0 & 8 \\ 3 & -1 & 6 \\ -2 & 0 & -5 \end{pmatrix}.$$

Trouver une base de $\mathbb{R}^3$ dans laquelle la matrice de f ait une forme réduite de Jordan.

Solution. On rappelle la méthode suivante pour trouver une forme réduite de Jordan ainsi que la base respective d'une application linéaire $f : E \to E$ sur un $\Bbbk$-espace vectoriel E de dimension finie, si telle forme existe.

(J.1) On calcule les valeurs propres de f, en calculant les racines du polynôme caractéristique χ_f de f. On suppose que l'ensemble de valeurs propres de f est donné par $\{\lambda_1, \dots, \lambda_r\}$, avec $\lambda_i \neq \lambda_j$ si $i, j \in [\![1, r]\!]$ sont différents.

(J.2) Pour chaque $i \in [\![1, r]\!]$, on calcule une base $\mathscr{B}_i = \{v_{i,1}, \dots, v_{i,\ell_i}\}$ du noyau $\mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f)$ contenant une base de $\mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f) \cap \mathsf{Img}(\lambda_i \,\mathsf{id}_V - f)^k$ pour tout $k \in [\![1, a_i - 1]\!]$, où a_i est la multiplicité de λ_i dans le polynôme caractéristique χ_f de f. On remarque $\mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f) \cap \mathsf{Img}(\lambda_i \,\mathsf{id}_V - f)^{a_i} = \{\mathbf{0}_V\}$. De façon explicite, pour trouver une telle base $\mathscr{B}_i$ on définit d'abord

$$k_0 = \max\left\{k \in [\![1, a_i - 1]\!] : \mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f) \cap \mathsf{Img}(\lambda_i \,\mathsf{id}_V - f)^k \neq \{\mathbf{0}_E\}\right\},$$

et pour tout $k \in [\![0, k_0]\!]$ on calcule une base $\tilde{\mathscr{B}}_{\lambda_i,k}$ d'un sous-espace vectoriel $F_{\lambda_i,k}$ qui satisfait que

$$F_{\lambda_i,k} \oplus \Big(\mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f) \cap \mathsf{Img}(\lambda_i \,\mathsf{id}_V - f)^{k+1}\Big) = \mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f) \cap \mathsf{Img}(\lambda_i \,\mathsf{id}_V - f)^k.$$

Alors, $\mathscr{B}_i = \cup_{k=0}^{k_0} \tilde{\mathscr{B}}_{\lambda_i,k}$ est une base du noyau $\mathsf{Ker}(\lambda_i \,\mathsf{id}_V - f)$ qui satisfait les propriétés demandées.

(J.3) Pour chaque $i \in [\![1, r]\!]$ et $j \in [\![1, \ell_i]\!]$, on construit une famille

$$\mathscr{B}_{i,j} = \{v_{i,j,1}, \dots, v_{i,j,N_{i,j}}\} \subseteq E \setminus \{\mathbf{0}_E\}$$

par récurrence de la façon suivante :

(i) $v_{i,j,1} = v_{i,j}$;
(ii) $v_{i,j,k}$ satisfait que $v_{i,j,k-1} = (f - \lambda_i \,\mathsf{id}_V)(v_{i,j,k})$ pour $k \in [\![2, N_{i,j}]\!]$;
(iii) $v_{i,j,N_{i,j}} \notin \mathsf{Img}(f - \lambda_i \,\mathsf{id}_V)$.

(J.4) Alors, la famille

$$\mathscr{B}_J = \bigcup_{i=1}^{r} \bigcup_{j=1}^{\ell_i} \mathscr{B}_{i,j}$$

est une base de E dont la représentation matricielle de f est une matrice de Jordan.

Dans ce cas, à partir de la représentation matricielle M de f, on voit que $\chi_f = (X+1)^3$, ce qui implique que l'ensemble de valeurs propres de f est $\{-1\}$. En outre, la même représentation matricielle M nous dit que $\dim(\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3} + f)) = 2$, vu que $\mathsf{I}_3 + M$ est équivalente par lignes à une matrice échelonnée en lignes avec 1 ligne non nulle. C'est facile à voir que $\{(2, 0, -1), (0, 1, 0)\}$ est une base de $\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3} - f)$. En outre, comme l'image de $\mathsf{id}_{\mathbb{R}^3}+f$ est $\mathsf{Vect}_{\mathbb{R}}\langle\{(4,3,-2)\}\rangle$, qui est trivialement incluse dans $\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3}+f)$, la base $\mathscr{B}=\{(0,1,0),(4,3,-2)\}$ de $\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3}+f)$ satisfait les conditions dans l'item (J.2). Dans ce cas $(0,1,0)\in\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3}+f)\setminus\mathsf{Img}(\mathsf{id}_{\mathbb{R}^3}+f)$ et

$$(4,3,-2)\in\big(\mathsf{Ker}(\mathsf{id}_{\mathbb{R}^3}+f)\cap\mathsf{Img}(\mathsf{id}_{\mathbb{R}^3}+f)\big)\setminus\mathsf{Img}((\mathsf{id}_{\mathbb{R}^3}+f)^2).$$

On note que $(\mathsf{id}_{\mathbb{R}^3}+f)(1,0,0)=(4,3,-2)$. D'après l'item (J.4), on obtient une base $\mathscr{B}_J=\{(0,1,0),(4,3,-2),(1,0,0)\}$ de $\mathbb{R}^3$, et la représentation matricielle de f dans la base $\mathscr{B}_J$ est

$$[f]_{\mathscr{B}_J}=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}.$$

18. Soit $\mathbb{C}[X]_{\leq 4}$ l'espace vectoriel de polynômes de degré inférieur ou égal à 4 à coefficients complexes et soit $f:\mathbb{C}[X]_{\leq 4}\to\mathbb{C}[X]_{\leq 4}$ l'application linéaire définie par $f(P)=2P(X+1)-P(X+2)$ pour $P\in\mathbb{C}[X]_{\leq 4}$. Trouver une base de $\mathbb{C}[X]_{\leq 4}$ dans laquelle la matrice de f ait une forme réduite de Jordan.

Solution. Soit $\mathscr{B}_c=\{1,X,X^2,X^3,X^4\}$ la base canonique de $\mathbb{C}[X]_{\leq 4}$. Alors, la représentation matricielle de f dans la base $\mathscr{B}_c$ est

$$[f]_{\mathscr{B}_c}=\begin{pmatrix}1&0&-2&-6&-14\\0&1&0&-6&-24\\0&0&1&0&-12\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}. \tag{15}$$

Dans ce cas, à partir de la représentation matricielle (15), on voit que $\chi_f=(X-1)^5$, ce qui implique que l'ensemble de valeurs propres de f est $\{1\}$. En outre, la même représentation matricielle (15) nous dit que $\dim(\mathsf{Ker}(\mathsf{id}_{\mathbb{C}[X]_{\leq 4}}-f))=2$, vu que $\mathsf{I}_5-[f]_{\mathscr{B}_c}$ est équivalente par lignes à une matrice échelonnée en lignes avec 3 lignes non nulles. C'est facile à voir que $\{X,1\}$ est une base de $\mathsf{Ker}(\mathsf{id}_{\mathbb{C}[X]_{\leq 4}}-f)$. Pour le vecteur propre X, en employant la représentation matricielle (15), on trouve que $(f-\mathsf{id}_{\mathbb{C}[X]_{\leq 4}})(-X^3/6+X^2/2)=X$ et il n'existe pas de $P\in\mathbb{C}[X]_{\leq 4}$ tel que $(f-\mathsf{id}_{\mathbb{C}[X]_{\leq 4}})(P)=-X^3/6+X^2/2$. De façon analogue, pour le vecteur propre 1, en employant la représentation matricielle (15), on trouve que $(f-\mathsf{id}_{\mathbb{C}[X]_{\leq 4}})(-X^2/2)=1$, $(f-\mathsf{id}_{\mathbb{C}[X]_{\leq 4}})(X^4/24-X^3/6+5X^2/24)=-X^2/2$ et il n'existe pas de $P\in\mathbb{C}[X]_{\leq 4}$ tel que $(f-\mathsf{id}_{\mathbb{C}[X]_{\leq 4}})(P)=X^4/24-X^3/6+5X^2/24$. On conclut alors que

$$\mathscr{B}_J=\{X,-X^3/6+X^2/2,1,-X^2/2,X^4/24-X^3/6+5X^2/24\}$$

est une base de Jordan de f, dont la représentation matricielle est

$$[f]_{\mathscr{B}_J}=\begin{pmatrix}1&1&0&0&0\\0&1&0&0&0\\0&0&1&1&0\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}.$$

19. Soit $\Bbbk$ un corps de caractéristique zéro et soient a et b dans $\Bbbk$. Donner la décomposition de Dunford de la matrice

$$M = \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}.$$

Solution. On rappelle que la décomposition de Dunford de M est l'expression $M = M_s + M_n$, où M_s est diagonalisable, M_n est nilpotent, et M_s et M_n commutent. Elle est unique. Si $a = b$, alors

$$M_s = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ et } M_n = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

tandis que si $a \neq b$, alors M est diagonalisable, ce qui implique que $M_s = M$ et $M_n = \mathbf{0}_{\mathsf{M}_{2\times 2}(\Bbbk)}$.

20. Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ l'endomorphisme linéaire dont la matrice dans la base canonique (e_1, e_2, e_3) est

$$M = \begin{pmatrix} 0 & -2 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

(a) Calculer le polynôme minimal μ_{f,e_i} associé au vecteur e_i pour $i \in \{1, 2, 3\}$.

(b) En déduire le polynôme minimal $\mu_{f,\mathbb{R}}$ et le polynôme caractéristique χ_f.

(c) Soit $\psi : \mathbb{R}[X] \to L(\mathbb{R}^3)$ le morphisme d'anneaux défini par $\psi(P) = P(f)$ pour $P \in \mathbb{R}[X]$.

(i) Quel est le noyau de ψ ?

(ii) On note $B = \mathsf{Img}(\psi)$. C'est clairement un sous-anneau et aussi un sous-espace vectoriel de $\mathsf{L}(\mathbb{R}^3)$. Quelle est sa dimension comme espace vectoriel sur $\mathbb{R}$?

(iii) L'anneau B est-il intègre ?

(iv) L'endomorphisme f est-il un élément inversible de l'anneau B ?

(d) Montrer que l'anneau $\mathbb{R}[X]/(X^2 + 2X + 2)$ est isomorphe au corps $\mathbb{C}$.

(e) Montrer qu'il existe un unique morphisme d'anneaux $\gamma : B \to \mathbb{C} \times \mathbb{R}$ tel que $\gamma(f) = (i - 1, 5)$.

(f) Vérifier que γ est $\mathbb{R}$-linéaire et bijective.

Solution.

(a) On voit bien que $f(e_1) = e_2$, $f^2(e_1) = -2e_1 - 2e_2$. Comme

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f)(e_1) = c_0 e_1 + c_1 e_2$$

implique forcément $c_0 = c_1 = 0$, $\deg(\mu_{f,e_1}) > 1$. En outre,

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f + f^2)(e_1) = (c_0 - 2)e_1 + (c_1 - 2)e_2$$

implique $c_0 = c_1 = 2$, *i.e.* $(f^2 + 2f + 2\,\mathsf{id}_{\mathbb{R}^3}(e_1) = \mathbf{0}_{\mathbb{R}^3}$. En conséquence, $\mu_{f,e_1} = X^2 + 2X + 2$.

De la même façon, on voit bien que $f(e_2) = -2e_1 - 2e_2$, $f^2(e_2) = 4e_1 + 2e_2$. Comme

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f)(e_2) = -2c_1 e_1 + (c_0 - 2c_1)e_2,$$

implique forcément $c_0 = c_1 = 0$, $\deg(\mu_{f,e_2}) > 1$. En outre,

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f + f^2)(e_2) = (4 - 2c_1)e_1 + (c_0 - 2c_1 + 2)e_2,$$

implique $c_0 = c_1 = 2$, *i.e.* $(f^2 + 2f + 2\,\mathsf{id}_{\mathbb{R}^3}(e_2) = \mathbf{0}_{\mathbb{R}^3}$. En conséquence, $\mu_{f,e_2} = X^2 + 2X + 2$.

Finalement, comme $f(e_3) = e_3$, $\mu_{f,e_3} = X - 5$.

(*b*) En employant l'item (g) de l'exercice **12** on voit que

$$\mu_{f,\mathbb{R}} = \mathsf{PPCM}(X^2 + 2X + 2, X - 5) = (X^2 + 2X + 2)(X - 5) = X^3 - 3X^2 - 8X - 10,$$

vu que X^2+2X+2 et $X-5$ sont premiers entre eux, car 5 n'est pas une racine X^2+2X+2. Comme $\mu_{f,\mathbb{R}} | \chi_f$, vu que $\chi_f(f) = \mathbf{0}_{\mathsf{L}(\mathbb{C}^3)}$, et $\deg(\chi_f) = 3 = \deg(\mu_{f,\mathbb{R}})$, on conclut que $\chi_f = \mu_{f,\mathbb{R}}$, car les deux polynômes sont unitaires.

(*c*) (i) Par définition, le noyau de ψ est l'idéal de $\mathbb{R}[X]$ engendré par le polynôme minimal $\mu_{f,\mathbb{R}} = (X^2 + 2X + 2)(X - 5)$.

(ii) D'après le premier théorème d'isomorphisme d'anneaux on a un morphisme injectif d'anneaux $\mathbb{R}[X]/(\mu_{f,\mathbb{R}}) \to \mathsf{L}(\mathbb{R}^3)$ d'image B. Cette application est aussi linéaire. Comme $\dim(\mathbb{R}[X]/(\mu_{f,\mathbb{R}})) = \deg(\mu_{f,\mathbb{R}}) = 2$, B a dimension 2.

(iii) L'anneau $\mathbb{R}[X]/(\mu_{f,\mathbb{R}}) \simeq B$ n'est pas intègre, car

$$\overline{X^2 + 2X + 2}.\overline{X - 5} = \overline{(X^2 + 2X + 2)(X - 5)} = \mathbf{0}_{\mathbb{R}[X]/(\mu_{f,\mathbb{R}})}$$

mais les deux facteurs du premier membre ne sont pas nuls.

(iv) Comme $\mu_{f,\mathbb{R}} = X^3 - 3X^2 - 8X - 10$, $f^3 - 3f^2 - 8f - 10\,\mathsf{id}_{\mathbb{R}^3} = \mathbf{0}_{\mathsf{L}(\mathbb{R}^3)}$, ce qui implique que

$$(f^2/10 - 3f/10 - 2\,\mathsf{id}_{\mathbb{R}^3}/5) \circ f = f \circ (f^2/10 - 3f/10 - 2\,\mathsf{id}_{\mathbb{R}^3}/5) = \mathsf{id}_{\mathbb{R}^3},$$

$f^2/10 - 3f/10 - 2\,\mathsf{id}_{\mathbb{R}^3}/5 \in B$ est l'inverse de f.

(*d*) On considère le morphisme d'anneaux $\mathsf{ev}_{i-1} : \mathbb{R}[X] \to \mathbb{C}$ qui associe $P(i-1)$ à $P \in \mathbb{R}[X]$. On voit bien que $\mathsf{ev}_{i-1}(X^2 + 2X + 2) = 0$, vu que les racines de $X^2 + 2X + 2$ sont $-1 - i$ et $-1 + i$. En conséquence, l'idéal $(X^2 + 2X + 2)$ engendré par $X^2 + 2X + 2$ est inclus dans le noyau $\mathsf{Ker}(\mathsf{ev}_{i-1})$, et ev_{i-1} induit un morphisme d'anneaux $\bar{\mathsf{ev}}_{i-1} : \mathbb{R}[X]/(X^2 + 2X + 2) \to \mathbb{C}$. Comme $\mathsf{ev}_{i-1} : \mathbb{R}[X] \to \mathbb{C}$ est surjectif, vu qu'il s'agit d'une application $\mathbb{R}$-linéaire, $\mathsf{ev}_{i-1}(1) = 1$ et $\mathsf{ev}_{i-1}(X + 1) = i$, $\bar{\mathsf{ev}}_{i-1}$ est aussi surjectif. L'identité $\dim_{\mathbb{R}}(\mathbb{R}[X]/(X^2 + 2X + 2)) = \dim_{\mathbb{R}}(\mathbb{C}) = 2$ nous dit alors que $\bar{\mathsf{ev}}_{i-1}$ est bijectif.

(*e*) Soit $\mathsf{ev}_{i-1,5} : \mathbb{R}[X] \to \mathbb{C} \times \mathbb{R}$ le morphisme d'anneaux donné par $\Gamma(P) = (P(i-1), P(5))$. On voit bien que $\mathsf{ev}_{i-1,5}(\mu_{f,\mathbb{R}}) = 0$, vu que les racines de $\mu_{f,\mathbb{R}} = (X^2 + 2X + 2)(X - 5)$ sont $-1 - i$, $-1 + i$ et 5. En conséquence, l'idéal $(\mu_{f,\mathbb{R}})$ engendré par $\mu_{f,\mathbb{R}}$ est inclus dans le noyau $\mathsf{Ker}(\mathsf{ev}_{i-1,5})$, et $\mathsf{ev}_{i-1,5}$ induit un morphisme d'anneaux $\bar{\mathsf{ev}}_{i-1,5} : \mathbb{R}[X]/(\mu_{f,\mathbb{R}}) \to \mathbb{C} \times \mathbb{R}$. On définit le morphisme d'anneaux $\gamma : B \to \mathbb{C} \times \mathbb{R}$ par $\gamma = \bar{\mathsf{ev}}_{i-1,5} \circ \hat{\psi}^{-1}$, où $\hat{\psi} : \mathbb{R}[X]/(\mu_{f,\mathbb{R}}) \to B$ est l'isomorphisme d'anneaux donné par la correstriction du morphisme ψ définie dans l'item (c). On voit bien que

$$\gamma(f) = (\bar{\mathsf{ev}}_{i-1,5} \circ \hat{\psi}^{-1})(f) = \bar{\mathsf{ev}}_{i-1,5}(\bar{X}) = \mathsf{ev}_{i-1,5}(X) = (i - 1, 5).$$

Pour prouver l'unicité de γ, il suffit de montrer que si $\gamma_1, \gamma_2 : B \to \mathbb{C} \times \mathbb{R}$ sont deux morphismes d'anneaux tels que $\gamma_1(f) = \gamma_2(f)$, alors $\gamma_1(b) = \gamma_2(b)$ pour tout $b \in B$. Cela suit du fait que pour tout $b \in B$ il existe $P \in \mathbb{R}[X]$ tel que $b = P(f)$ et

$$\gamma_1\big(P(f)\big) = P\big(\gamma_1(f)\big) = P\big(\gamma_2(f)\big) = \gamma_2\big(P(f)\big).$$

(*f*) On voit bien que γ est $\mathbb{R}$-linéaire, vu que les morphismes ψ et $\mathsf{ev}_{i-1,5}$ le sont. En outre, on voit que γ est surjectif, vu que $\gamma(\mathsf{id}_{\mathbb{R}^3}) = (1,1)$, $\gamma(\mathsf{id}_{\mathbb{R}^3}) = (1,1)$, $\gamma(f - 5\,\mathsf{id}_{\mathbb{R}^3}) = (i-6,0)$ et $\gamma(f^2 + 2f + 2\,\mathsf{id}_{\mathbb{R}^3}) = (0,37)$, et $\{(1,1),(i-6,0),(0,37)\}$ est une famille génératrice de l'espace vectoriel réel $\mathbb{C}\times\mathbb{R}$. L'identité $\dim_{\mathbb{R}}(B) = \dim_{\mathbb{R}}(\mathbb{R}[X]/(\mu_{f,\mathbb{R}})) = \dim_{\mathbb{R}}(\mathbb{C}\times\mathbb{R}) = 3$ nous dit alors que γ est bijectif.

21. Soit E un $\mathbb{R}$-espace vectoriel de dimension 3, muni d'une base $\mathscr{B} = (e_1,e_2,e_3)$.

(*a*) Soit $f : E \to E$ l'endomorphisme linéaire dont la matrice dans la base $\mathscr{B}$ est

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

(i) Calculer le polynôme minimal μ_{f,e_i} associé au vecteur e_i pour $i \in \{1,2,3\}$.

(ii) En déduire le polynôme minimal $\mu_{f,\mathbb{R}}$ et le polynôme caractéristique χ_f.

(*b*) Soit $h : E \to E$ un endomorphisme linéaire vérifiant $h^3 + h = \mathbf{0}_{\mathsf{L}(E)}$.

(i) Quelles sont les différentes possibilités pour le polynôme minimal $\mu_{h,\mathbb{R}}$ et pour le polynôme caractéristique χ_h d'un tel endomorphisme ?

(ii) Un tel endomorphisme h peut-il être injectif ?

(iii) Quelles sont les différentes possibilités pour la dimension du noyau de $h^2 + \mathsf{id}_E$?

(iv) Montrer que la matrice de h dans la base $\mathscr{B}$ est ou bien nulle ou bien semblable à la matrice A.

Solution.

(*a*) (i) On voit bien que $f(e_1) = \mathbf{0}_E$, ce qui implique que $\mu_{f,e_1} = X$.

En outre, on voit bien que $f(e_2) = e_3$ et $f^2(e_2) = -e_2$. Comme

$$\mathbf{0}_E = (c_0 + c_1 f)(e_2) = c_0 e_2 - c_1 e_3$$

implique forcément $c_0 = c_1 = 0$, $\deg(\mu_{f,e_2}) > 1$. En outre,

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f + f^2)(e_2) = (c_0 - 1)e_2 + c_1 e_2$$

implique $c_0 = 1$ et $c_1 = 0$, *i.e.* $(f^2 + \mathsf{id}_{\mathbb{R}^3}(e_2) = \mathbf{0}_E$. En conséquence, $\mu_{f,e_2} = X^2 + 1$.

Finalement, on voit bien que $f(e_3) = -e_2$ et $f^2(e_3) = -e_3$. Comme

$$\mathbf{0}_E = (c_0 + c_1 f)(e_3) = c_0 e_3 - c_1 e_2$$

implique forcément $c_0 = c_1 = 0$, $\deg(\mu_{f,e_3}) > 1$. En outre,

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f + f^2)(e_3) = (c_0 - 1)e_3 + c_1 e_2$$

implique $c_0 = 1$ et $c_1 = 0$, *i.e.* $(f^2 + \mathsf{id}_{\mathbb{R}^3}(e_3) = \mathbf{0}_E$. En conséquence, $\mu_{f,e_3} = X^2 + 1$.

(ii) En employant l'item (g) de l'exercice **12** on voit que

$$\mu_{f,\mathbb{R}} = \mathsf{PPCM}(X^2 + 1, X) = (X^2+1)X = X^3 + X,$$

vu que $X^2 + 1$ et X sont premiers entre eux, car 0 n'est pas une racine $X^2 + 1$. Comme $\mu_{f,\mathbb{R}} | \chi_f$, vu que $\chi_f(f) = \mathbf{0}_{\mathsf{L}(E)}$, et $\deg(\chi_f) = 3 = \deg(\mu_{f,\mathbb{R}})$, on conclut que $\chi_f = \mu_{f,\mathbb{R}}$, car les deux polynômes sont unitaires.

(b) (i) Par définition, $\mu_{h,\mathbb{R}}|(X^3+X)$, vu que $h^3+h = \mathbf{0}_{\mathsf{L}(E)}$. En conséquence, $\mu_{h,\mathbb{R}} \in \{X, X^2+1, X^3+X\}$, vu que $h \in \mathbb{R}[X]$ divise X^3+X dans $\mathbb{R}[X]$ et X^2+1 est irréductible dans $\mathbb{R}[X]$.

On affirme en plus que $\mu_{h,\mathbb{R}} \neq X^2+1$. Pour le montrer, on remarque d'ailleurs le fait élémentaire que dit que, étant donné une application linéaire $f \in \mathsf{L}(E)$ sur un $\Bbbk$-espace vectoriel de dimension finie, toute racine dans $\Bbbk$ du polynôme caractéristique χ_f est aussi une racine du polynôme minimal $\mu_{f,\Bbbk}$. En effet, $\lambda \in \Bbbk$ est racine du polynôme caractéristique χ_f si et seulement si λ est une valeur propre de f, *i.e.* il existe $v \in V$ non nul tel que $f(v) = \lambda v$. En conséquence, $\mu_{f,v} = X - \lambda$ et $\mu_{f,v}$ divise $\mu_{f,\Bbbk}$, ce qui implique que λ est une racine de $\mu_{f,\Bbbk}$. On va montrer maintenant que $\mu_{h,\mathbb{R}} \neq X^2+1$. On suppose que $\mu_{h,\mathbb{R}} = X^2+1$. Comme $h \in \mathsf{L}(E)$, son polynôme caractéristique $\chi_f \in \mathbb{R}[X]$ a degré 3 et en conséquence au moins une racine réelle $\lambda \in \mathbb{R}$. D'après ce que l'on vient d'expliquer λ est une racine de $\mu_{h,\mathbb{R}} = X^2+1$. Comme ce dernier polynôme n'a pas de racines réelles, on trouve un absurde, ce qui implique que $\mu_{h,\mathbb{R}} \neq X^2+1$.

On remarque en outre que les possibilités $\{X, X^3+X\}$ sont vraiment atteintes, car si $h = \mathbf{0}_{\mathsf{L}(E)}$, alors $\mu_{h,\mathbb{R}} = X$, et si $h = f$ alors $\mu_{h,\mathbb{R}} = X^3+X$.

Finalement, si $\mu_{h,\mathbb{R}} = X$ alors $h = \mathbf{0}_{\mathsf{L}(E)}$, ce qui implique que $\chi_h = X^3$, et si $\mu_{h,\mathbb{R}} = X^3+X$, comme $\mu_{h,\mathbb{R}}|\chi_h$, alors $\chi_h = X^3+X$. En conséquence, $\chi_h \in \{X^3, X^3+X\}$ et toutes les possibilités sont atteintes.

(ii) Si $\mu_{h,\mathbb{R}} = X$ alors $h = \mathbf{0}_{\mathsf{L}(E)}$, ce qui implique que h n'est pas injectif. Si $\mu_{h,\mathbb{R}} = X^3+X$, alors 0 est une valeur propre de h de multiplicité 1, ce qui nous dit que h n'est pas injectif et $\mathsf{dim}(\mathsf{Ker}(h)) = 1$. En conséquence, h n'est jamais injectif.

(iii) Si $\mu_{h,\mathbb{R}} = X$ alors $h = \mathbf{0}_{\mathsf{L}(E)}$, ce qui implique que $h^2 + \mathsf{id}_E = \mathsf{id}_E$ est injectif, et en particulier son noyau est $\{\mathbf{0}_E\}$, qui a dimension 0.

Si $\mu_{h,\mathbb{R}} = X^3+X$, alors $h^2 + \mathsf{id}_E \neq \mathbf{0}_{\mathsf{L}(E)}$, ce qui implique que $\mathsf{dim}(\mathsf{Ker}(h^2+\mathsf{id}_E)) < \mathsf{dim}(E) = 3$. Comme $\mathsf{dim}(\mathsf{Ker}(h)) = 1$, $\mathsf{dim}(\mathsf{Img}(h)) = \mathsf{dim}(E) - \mathsf{dim}(\mathsf{Ker}(h)) = 2$. L'inclusion évidente $\mathsf{Img}(h) \subseteq \mathsf{Ker}(h^2+\mathsf{id}_E)$ (qui suit du fait que $(h^2+\mathsf{id}_E)\circ h = \mathbf{0}_{\mathsf{L}(E)}$) nous dit alors que

$$2 = \mathsf{dim}(\mathsf{Img}(h)) \leq \mathsf{dim}(\mathsf{Ker}(h^2+\mathsf{id}_E)) \leq 2,$$

i.e. $\mathsf{Ker}(h^2+\mathsf{id}_E)$ a dimension 2.

(iv) Si $\mu_{h,\mathbb{R}} = X$ alors $h = \mathbf{0}_{\mathsf{L}(E)}$, ce qui implique que la matrice de h dans la base $\mathscr{B}$ est nulle. Si $\mu_{h,\mathbb{R}} = X^3+X$, alors 0 est une valeur propre de h de multiplicité 1. Soit $v_1 \in E$ non nul tel que $h(v_1) = \mathbf{0}_E$. Soit $v_2 \in \mathsf{Ker}(h^2+\mathsf{id}_E)$ non nul. On remarque $\mathsf{Ker}(h^2+\mathsf{id}_E) \cap \mathsf{Ker}(h) = \{\mathbf{0}_E\}$, car si $v \in \mathsf{Ker}(h^2+\mathsf{id}_E)\cap\mathsf{Ker}(h)$ on a alors $\mathbf{0}_E = (h^2+\mathsf{id}_E)(v) = h^2(v)+v = \mathbf{0}_E + v = v$. Alors $v_3 = h(v_2) \in \mathsf{Ker}(h^2+\mathsf{id}_E)$ est non nul. On voit bien que $\mathscr{B}' = \{v_1, v_2, v_3\}$ est une famille libre de E, et en conséquence une base de E. Pour le montrer, il suffit de montrer que v_3 n'est pas un multiple de v_2. Si $v_3 = \lambda v_2$ avec $\lambda \in \mathbb{R}$ non nul, alors $h(v_2) = v_3 = \lambda v_2$, ce qui implique que λ est une valeur propre réelle non nulle de f, ce qui est impossible. On note en plus que $h(v_3) = h^2(v_2) = -v_2$. En conséquence, la matrice de h relative à la base $\mathscr{B}'$ est

$$[h]_{\mathscr{B}'} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Soit P la matrice de passage de la base $\mathscr{B}$ dans la base $\mathscr{B}'$. On a alors $[h]_{\mathscr{B}} = P[h]_{\mathscr{B}'}P^{-1}$. En conséquence, $[h]_{\mathscr{B}}$ est semblable à la matrice $A = [h]_{\mathscr{B}'}$.

22. (a) Soit $S = a_0 + a_1X + \cdots + a_dX^d$ un polynôme de $\mathbb{Z}[X]$ de degré $d \in \mathbb{N}^*$. Soient $p \in \mathbb{Z} \setminus \{0\}$ et $q \in \mathbb{N}^*$ premiers entre eux, et $r = p/q$. Montrer que si r est racine de S, alors q divise a_d et que p divise a_0 dans $\mathbb{Z}$.

(b) On fixe désormais $S = X^3 + X + 1$. Montrer que le polynôme S est irréductible dans $\mathbb{Q}[X]$.

(c) On note L l'anneau quotient $\mathbb{Q}[X]/(S)$. Montrer que L est un corps.

(d) On considère le $\mathbb{Q}$-espace vectoriel $E_1 = \mathbb{Q}^3$, et un endomorphisme linéaire $f : E_1 \to E_1$ tel que $f^3 + f + \mathrm{id}_{E_1} = \mathbf{0}_{\mathsf{L}(E_1)}$. Quel est le polynôme minimal de f ?

(e) Montrer que l'on peut définir une structure de L-espace vectoriel sur E_1 en définissant une loi externe par $\bar{P}.v = P(f)(v)$, pour tout $P \in \mathbb{Q}[X]$ et $v \in E_1$.

(f) Montrer qu'il existe une base du $\mathbb{Q}$-espace vectoriel E_1 dans laquelle la matrice de f est

$$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

(g) Quelle est la dimension de E_1 en tant que L-espace vectoriel ?

(h) On considère le $\mathbb{Q}$-espace vectoriel $E_2 = \mathbb{Q}^6$ et un endomorphisme $f : E_2 \to E_2$ tel que $h^3 + h + \mathrm{id}_{E_2} = \mathbf{0}_{\mathsf{L}(E_2)}$. Quel est le polynôme minimal de h ?

(i) Montrer que l'on peut définir une structure de L-espace vectoriel sur E_2 en définissant une loi externe par $\bar{P}.v = P(h)(v)$, pour tout $P \in \mathbb{Q}[X]$ et $v \in E_2$.

(j) Quelle est la dimension de E_2 en tant que L-espace vectoriel ?

(k) Montrer que tout endomorphisme g du $\mathbb{Q}$-espace vectoriel E_2 vérifiant l'identité $g^3 + g + \mathrm{id}_{E_2} = \mathbf{0}_{\mathsf{L}(E_2)}$ est un conjugué de h.

Solution.

(a) On voit bien que

$$q^d S(r) = q^d S\left(\frac{p}{q}\right) = \sum_{i=0}^{d} a_i p^i q^{d-i} = a_0 q^d + pq \sum_{i=1}^{d-1} a_i p^{i-1} q^{d-i-1} + a_d p^d,$$

ce qui implique que, si $r = p/q$ est une racine de S, alors p divise a_0 et q divise a_d.

(b) L'item précédent nous dit que S ne possède pas de racines dans $\mathbb{Q}$, vu que $S(1) = 3 \neq 0$ et $S(-1) = 1 \neq 0$. Comme tout polynôme $P \in \Bbbk[X]$ non nul de degré inférieur ou égal à 3 sans racines dans $\Bbbk$ est irréductible, où $\Bbbk$ est un corps, on conclut que S est irréductible dans $\mathbb{Q}[X]$.

(c) On remarque que, si $\Bbbk$ est un corps, tout polynôme $P \in \Bbbk[X]$ irréductible est premier, *i.e.* $\Bbbk[X]/(P)$ est intègre et non réduit à zéro. En effet, étant donné $Q_1, Q_2 \in \Bbbk[X]$ tels que $P|(Q_1Q_2)$, on va montrer que $P|Q_1$ ou $P|Q_2$. Si $P \nmid Q_1$, alors $\mathsf{PGCD}(P, Q_1) = 1$ vu que P est irréductible, ce qui implique qu'il existe $T_1, T_2 \in \Bbbk[X]$ tels que $1 = T_1P + T_2Q_1$, et en particulier $Q_2 = T_1PQ_2 + T_2Q_1Q_2$. Comme P divise T_1PQ_2 et Q_1Q_2, alors P divise Q_2.

En outre, on remarque que toute $\Bbbk$-algèbre A de dimension finie sur un corps $\Bbbk$ et intègre est une corps. En effet, pour tout $a \in A$ non nul, les applications $L_a, R_a : A \to A$ données par $L_a(x) = ax$ et $R_a(x) = xa$ pour tout $x \in A$ sont $\Bbbk$-linéaires et injectives. Comme A est de dimension finie sur $\Bbbk$, L_a et R_a sont bijectives, ce qui implique qu'il existe $b, c \in A$ tels que $ab = L_a(b) = 1_A = R_a(c) = ca$. En plus, $b = c$ vu que

$b = 1_A b = cab = c1_A = c$, ce qui implique que a est inversible et, en conséquence, A est un corps.

Finalement, comme S est irréductible dans $\mathbb{Q}[X]$, il est premier, ce qui nous dit que $\mathbb{Q}[X]/(S)$ est intègre. En plus, comme $\mathbb{Q}[X]/(S)$ est intègre et de dimension finie sur $\mathbb{Q}$, $\mathbb{Q}[X]/(S)$ est un corps.

(d) Comme $f^3 + f + \mathrm{id}_{E_1} = \mathbf{0}_{\mathsf{L}(E_1)}$, $\mu_{f,\mathbb{Q}}$ divise $X^3 + X + 1$. En plus, comme $X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ et $\deg(\mu_{f,\mathbb{Q}}) > 1$, $\mu_{f,\mathbb{Q}} = X^3 + X + 1$, car les deux polynômes sont unitaires.

(e) On rappelle qu'une structure de $\Bbbk$-espace vectoriel sur V est défini de façon équivalente par une structure de groupe abélien sur V et un morphisme d'anneaux $\rho : \Bbbk \to \mathsf{End}_{\mathsf{Gr}}(V)$, où $\mathsf{End}_{\mathsf{Gr}}(V) = \mathsf{Hom}_{\mathsf{Gr}}(V, V)$ est un anneau pour la somme usuelle de fonctions et le produit donné par composition.

Soit V un espace vectoriel de dimension finie sur $\Bbbk$ et soit $\phi \in \mathsf{L}(V)$ un endomorphisme $\Bbbk$-linéaire. On considère le morphisme d'anneaux $\mathsf{ev}_\phi : \Bbbk[X] \to \mathsf{L}(V) \subseteq \mathsf{End}_{\mathsf{Gr}}(V)$ qui associe $P(\phi)$ à $P \in \Bbbk[X]$. Alors, par définition, $\mathsf{Ker}(\mathsf{ev}_\phi)$ est un idéal engendré par $\mu_{\phi,\Bbbk}$, ce qui implique que ev_ϕ induit un morphisme injectif d'anneaux $\mathsf{ev}_\phi : \Bbbk[X]/(\mu_{\phi,\Bbbk}) \to \mathsf{L}(V) \subseteq \mathsf{End}_{\mathsf{Gr}}(V)$ d'après le premier théorème d'isomorphisme. Si l'on suppose en plus que $\mu_{f,\Bbbk}$ est irréductible dans $\Bbbk[X]$, $\Bbbk[X]/(\mu_{\phi,\Bbbk})$ est un corps d'après l'argument expliqué dans l'item (b), ce qui implique que V est un L-espace vectoriel. En plus, on remarque que $\mathsf{dim}_{\mathbb{Q}}(V) = \mathsf{dim}_{\mathbb{Q}}(L).\mathsf{dim}_L(V)$, ce qui implique que V est un L-espace vectoriel de dimension finie. De façon réciproque, si $P \in \Bbbk[X]$ est un polynôme irréductible, $L = \Bbbk[X]/(P)$ et V est un L-espace vectoriel de dimension finie, il existe un morphisme d'anneaux $\tau : L \to \mathsf{L}(V) \subseteq \mathsf{End}_{\mathsf{Gr}}(V)$ qui détermine la structure de L-espace vectoriel. Alors $\phi = \tau(\bar{X}) \in \mathsf{L}(V)$ est une application $\Bbbk$-linéaire de V, qui satisfait que $P(\phi) = \mathbf{0}_{\mathsf{L}(V)}$, ce qui implique que $\mu_{\phi,\Bbbk} | P$ dans $\Bbbk[X]$. Comme $\mu_{\phi,\Bbbk}$ et P sont irréductibles et unitaires, $\mu_{\phi,\Bbbk} = P$. En conclusion, pour un polynôme irréductible $P \in \Bbbk[X]$ fixe, il existe une bijection entre les couples (V, ϕ) avec V un espace vectoriel de dimension finie sur $\Bbbk$, $\phi \in \mathsf{L}(V)$ un endomorphisme $\Bbbk$-linéaire tel que $\mu_{\phi,\Bbbk} = P$, et les L-espaces vectoriels V de dimension finie avec $L = \Bbbk[X]/(P)$.

L'argument précédent nous dit que E_1 est L-espace vectoriel. C'est immédiat que cette structure de L-espace vectoriel est celle proposée dans l'énoncé.

(f) Soit $v \in E$ non nul et soit $\mathscr{B} = \{v, f(v), f^2(v)\}$. On affirme que $\mathscr{B}$ est libre sur $\mathbb{Q}$. En effet, soient $c_0, c_1, c_2 \in \mathbb{Q}$ tels que $c_0 v + c_1 f(v) + c_2 f^2(v) = \mathbf{0}_{E_1}$. Alors, $P = c_0 + c_1 X + c_2 X^2 \in \mathbb{Q}[X]$ est divisible par $\mu_{f,v}$. Comme $\deg(\mu_{f,v}) > 1$, $\mu_{f,v}$ divise $\mu_{f,\mathbb{Q}} = X^3 + X + 1$ et $X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$, $\mu_{f,v} = \mu_{f,\mathbb{Q}} = X^3 + X + 1$. En conséquence, comme $\deg(P) \leq 2$ et $\mu_{f,v}$ divise P, $P = \mathbf{0}_{\mathbb{Q}[X]}$, ce qui implique $c_0 = c_1 = c_2 = 0$. Comme $\mathscr{B} = \{v, f(v), f^2(v)\}$ est libre et $\mathsf{dim}_{\mathbb{Q}}(E_1) = 3$, $\mathscr{B}$ est une base de E_1. La matrice de h dans la base $\mathscr{B}$ est

$$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix},$$

vu que $f(f^2(v)) = -f(v) - v$.

(g) La dimension de E_1 comme L-espace vectoriel est 1. En effet, on rappelle que si V est L-espace vectoriel, alors $\mathsf{dim}_{\mathbb{Q}}(V) = \mathsf{dim}_{\mathbb{Q}}(L).\mathsf{dim}_L(V)$. En conséquence, $3 = \mathsf{dim}_{\mathbb{Q}}(E_1) = 3.\mathsf{dim}_L(E_1)$ implique que $\mathsf{dim}_L(E_1) = 1$.

(h) Comme $h^3 + h + \mathrm{id}_{E_2} = \mathbf{0}_{\mathsf{L}(E_2)}$, $\mu_{h,\mathbb{Q}}$ divise $X^3 + X + 1$. En plus, comme $X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ et $\deg(\mu_{h,\mathbb{Q}}) > 1$, $\mu_{h,\mathbb{Q}} = X^3 + X + 1$, car les deux polynômes sont unitaires.

(i) L'argument dans l'item (d) nous dit que E_2 est L-espace vectoriel. C'est immédiat que cette structure de L-espace vectoriel est celle proposée dans l'énoncé.

(j) La dimension de E_2 comme L-espace vectoriel est 2. En effet, comme $\dim_{\mathbb{Q}}(V) = \dim_{\mathbb{Q}}(L).\dim_L(V)$ pour V un L-espace vectoriel, alors

$$6 = \dim_{\mathbb{Q}}(E_2) = 3.\dim_L(E_2)$$

implique que $\dim_L(E_2) = 2$.

(k) Comme on a expliqué dans l'item (d), un endomorphisme $\phi \in \mathsf{L}(V)$ tel que $\phi^3 + \phi + \mathrm{id}_V = \mathbf{0}_{\mathsf{L}(V)}$ est équivalent à une structure de L-espace vectoriel sur V, que l'on notera V_ϕ. En particulier $(E_2)_h$ et $(E_2)_g$ sont deux structures de L-espace vectoriel définies sur E_2. Comme ils ont la même dimension sur L, il existe un isomorphisme L-linéaire $\psi : (E_2)_h \to (E_2)_g$, qui est à fortiori $\mathbb{Q}$-linéaire. La L-linéarité de ψ nous dit en particulier que $\psi(h(v)) = g(\psi(v))$ pour tout $v \in E_2$, ce qui équivaut à $h = \psi^{-1} \circ\circ g \circ \psi$, *i.e.* h et g sont conjugués.

23. Soit $f : \mathbb{C}^3 \to \mathbb{C}^3$ l'endomorphisme linéaire dont la matrice dans la base canonique (e_1, e_2, e_3) est

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}.$$

(a) Calculer μ_{f,e_1}.

(b) En déduire $\mu_{f,\mathbb{C}}$ et χ_f.

(c) Calculer le polynôme dérivé χ_f'.

(d) Calculer le PGCD des polynômes χ_f et χ_f'.

(e) En déduire que l'endomorphisme f est diagonalisable.

Solution.

(a) Un calcul directe nous dit que $\chi_f = X^3 - 3X^2 + 3X - 3$. Par ailleurs, on voit bien que $f(e_1) = e_1 + e_3$, $f^2(e_1) = e_1 + 2e_2 + 2e_3$ et $f^3(e_1) = 3e_1 + 6e_2 + 3e_3$. En particulier,

$$\mathbf{0}_{\mathbb{C}^3} = (c_0 + c_1 f + c_2 f^2)(e_1) = (c_0 + c_1 + c_2)e_1 + 2c_2 e_2 + (c_1 + 2c_2)e_3$$

implique forcément $c_0 = c_1 = c_2 = 0$, ce qui nous dit que $\deg(\mu_{f,e_1}) > 2$. En outre, comme $\mu_{f,e_1} | \chi_f$, vu que $\chi_f(f) = \mathbf{0}_{\mathsf{L}(\mathbb{C}^3)}$, on conclut que $\mu_{f,e_1} = \chi_f = X^3 - 3X^2 + 3X - 3$.

(b) Comme μ_{f,e_1} divise $\mu_{f,\mathbb{C}}$, qui divise aussi $\chi_f = X^3 - 3X^2 + 3X - 3$, et $\mu_{f,e_1} = \chi_f$, on conclut que $\mu_{f,e_1} = \mu_{f,\mathbb{C}} = \chi_f = X^3 - 3X^2 + 3X - 3$:

(c) Un calcul direct nous dit que $\chi_f' = 3X^2 - 6X + 3 = 3(X-1)^2$.

(d) Comme 1 n'est pas racine de $\chi_f = X^3 - 3X^2 + 3X - 3$, vu que $\chi_f(1) = -2 \neq 0$, et 1 est la seule racine de χ_f', on conclut que χ_f et χ_f' sont premier entre eux.

(e) L'item précédent nous dit que toutes les racines de χ_f sont simples, ce qui implique que f est diagonalisable.

Endomorphismes des espaces euclidiens*

* **24.** Soit E un espace vectoriel muni d'une forme bilinéaire symétrique non dégénérée $b = \langle \cdot, \cdot \rangle$. Soit j l'application de E dans E^* définie par $j(x) = \langle x, \cdot \rangle$.

(*a*) Montrer que j est un isomorphisme de E sur E^*.

(*b*) Soit $\mathscr{B}$ une base de E. À quelle condition la base $j(\mathscr{B})$ est-elle duale de $\mathscr{B}$?

(*c*) Montrer que pour tout sous-espace F de E, l'orthogonal $F^{\perp} \subseteq E^*$ de F dans E^* coïncide avec l'image par j de l'orthogonal

$$F^{\perp,b} = \{w \in E : \langle w, v \rangle = 0 \text{ pour tout } v \in F\}$$

de F dans E.

(*d*) Soit $u \in \mathsf{L}(E)$. Montrer que l'**adjoint** de u relatif à b est donné par

$$u^*(x) = j^{-1}(j(x) \circ u),$$

pour tout $x \in E$, et que ${}^{\mathrm{t}}u = j \circ u^* \circ j^{-1}$. Dans une base orthonormée de E, quelle relation y a-t-il entre la matrice de u^* et celle de u ?

Solution.

(*a*) Il s'agit d'un conséquence de l'exercice **2**, (b), car $\langle \cdot, \cdot \rangle$ est une forme bilinéaire non dégénérée. Noter que, en particulier, E est de dimension finie.

(*b*) C'est clair que $j(\mathscr{B})$ est la base duale de $\mathscr{B}$ si et seulement si $\langle v, w \rangle = j(v)(w) = \delta_{v,w}$ pour tous $v, w \in \mathscr{B}$, ce qui équivaut à dire que $\mathscr{B}$ est un base orthonormée de E pour $\langle \cdot, \cdot \rangle$.

(*c*) C'est clair que $j(F^{\perp,b}) \subseteq F^{\perp}$, vu que, étant donné $w \in F^{\perp,b}$, $j(w)(v) = \langle w, v \rangle = 0$ pour tout $v \in F$ nous dit que $j(w) \in F^{\perp}$. De façon réciproque, si $\varphi \in F^{\perp}$, comme j est un isomorphisme, il existe $w \in E$ tel que $\varphi = j(w)$. Or, l'identité $\langle w, v \rangle = j(w)(v) = 0$ pour tout $v \in F$ nous dit que $w \in F^{\perp,b}$. En conséquence, $j(F^{\perp,b}) \supseteq F^{\perp}$. On conclut que $j(F^{\perp,b}) = F^{\perp}$.

(*d*) On rappelle que l'adjoint de u relatif à b est l'unique application linéaire $u^* \in \mathsf{L}(E)$ qui satisfait que $\langle u(v), w \rangle = \langle v, u^*(w) \rangle$ pour tous $v, w \in E$. Comme $\langle v, j^{-1}(\varphi) \rangle = \varphi(v)$ pour tout $v \in E$ et $\varphi \in E^*$, on voit bien que

$$\langle v, j^{-1}(j(w) \circ u) \rangle = (j(w) \circ u)(v) = j(w)\big(u(v)\big) = \langle w, u(v) \rangle = \langle u(v), w \rangle = \langle v, u^*(w) \rangle$$

pour tous $v, w \in E$. En conséquence, $u^*(w) = j^{-1}(j(w) \circ u)$ pour tout $w \in E$. En outre, ${}^{\mathrm{t}}u = j \circ u^* \circ j^{-1}$ équivaut à démontrer ${}^{\mathrm{t}}u \circ j = j \circ u^*$, *i.e.* ${}^{\mathrm{t}}u \circ j(w) = j \circ u^*(w)$ pour tout $w \in E$, qui est équivalente à $({}^{\mathrm{t}}u \circ j(w))(v) = (j \circ u^*(w))(v)$ pour tous $v, w \in E$, ce qui suit directement de

$$({}^{\mathrm{t}}u \circ j(w))(v) = j(w)(u(v)) = \langle u(v), w \rangle = \langle u^*(w), v \rangle = (j \circ u^*(w))(v).$$

Finalement, on note que si $\mathscr{B} = \{v_1, \dots, v_n\}$ est une base orthonormée de E pour b, alors

$$[u^*]_{\mathscr{B}\mathscr{B}} = {}^{\mathrm{t}}[u]_{\mathscr{B}\mathscr{B}}, \tag{16}$$

vu que

$$u(v_j) = \sum_{i=1}^{n} c_{i,j} v_i \text{ et } u^*(v_j) = \sum_{i=1}^{n} d_{i,j} v_i$$

nous disent que $c_{i,j} = \langle u(v_j), v_i \rangle$ et $d_{i,j} = \langle u^*(v_j), v_i \rangle$ pour tous $i, j \in [\![1, n]\!]$. Comme $c_{i,j} = \langle u(v_j), v_i \rangle = \langle u^*(v_i), v_j \rangle = d_{j,i}$, on trouve (16).

⋆ **25.** Soit E un espace euclidien orienté de dimension 3. On note $\langle\,,\rangle : E \times E \to \mathbb{R}$ le produit scalaire. Pour tous vecteurs x, y, z, on note $[x, y, z]$ le produit mixte de x, y, z, défini comme le déterminant de (x, y, z) dans n'importe quelle base orthonormée directe de E. Noter que cela ne dépend pas du choix de la base orthonormée directe. On rappelle que l'application de E^3 dans $\mathbb{R}$ donnée par $(x, y, z) \mapsto [x, y, z]$ est trilinéaire alternée, donc antisymétrique. Pour tous vecteurs u et v de E, il existe un unique vecteur noté $u \wedge v$ tel que la forme linéaire $[u, v, \cdot]$ soit égale au produit scalaire par $u \wedge v$, *i.e.* $[u, v, w] = \langle u \wedge v, w\rangle$ pour tous $u, v, w \in E$.

(a) Montrer que si (e_1, e_2, e_3) est une base orthonormée directe, alors $e_1 \wedge e_2 = e_3$. **Indication :** montrer que les formes linéaires $\langle e_1 \wedge e_2, \cdot\rangle$ et $\langle e_3, \cdot\rangle$ sont égales.

(b) Montrer que l'application $(u, v) \mapsto u \wedge v$ de E^2 dans E est bilinéaire.

(c) Soient u et v de E. Montrer que

(i) $v \wedge u = -u \wedge v$;

(ii) $u \wedge v$ est orthogonal à u et v ;

(iii) si u et v sont colinéaires, $u \wedge v = \mathbf{0}_E$;

(iv) si u et v ne sont pas colinéaires, $u \wedge v \neq \mathbf{0}_E$ et $[u, v, u\wedge v] > 0$ (*i.e.* $(u, v, u\wedge v)$ est une base directe de E) ;

(v) si l'on suppose que u et v ne sont pas nuls, montrer que l'on peut trouver une base orthonormée directe (e_1, e_2, e_3) et un réel $\theta \in [0, \pi]$ tels que $||u||^{-1}u = e_1$ et $||v||^{-1}v = \cos(\theta)e_1 + \sin(\theta)e_2$.

Calculer $\langle u, v\rangle$ pour vérifier que θ est l'écart angulaire entre u et v et montrer que $||u \wedge v|| = ||u||.||v||.\sin(\theta)$.

Solution.

(a) Soit $v = \sum_{i=1}^{3} c_i e_i$, avec $c_i \in \mathbb{R}$. On voit bien que

$$\langle e_1 \wedge e_2, v\rangle = \sum_{i=1}^{3} c_i \langle e_1 \wedge e_2, e_i\rangle = c_3\langle e_1 \wedge e_2, e_3\rangle = \sum_{i=1}^{3} c_i\langle e_3, e_i\rangle = \langle e_3, v\rangle,$$

où l'on a utilisé que (e_1, e_2, e_i) n'est pas libre si $i \in \{1, 2\}$. En conséquence, les formes linéaires $\langle e_1 \wedge e_2, \cdot\rangle$ et $\langle e_3, \cdot\rangle$ coïncident, ce qui nous dit que $e_1 \wedge e_2 = e_3$.

(b) On voit bien que

$$\begin{aligned}\langle u \wedge (v + \lambda v'), w\rangle &= [u, (v + \lambda v'), w] = [u, v, w] + \lambda[u, v', w]\\ &= \langle u \wedge v, w\rangle + \lambda\langle u \wedge v', w\rangle = \langle u \wedge v + \lambda u \wedge v', w\rangle\end{aligned}$$

pour tous $u, v, v', w \in E$ et $\lambda \in \mathbb{R}$, ce qui implique que $u \wedge (v + \lambda v') = u \wedge v + \lambda u \wedge v'$ pour tous $u, v, v' \in E$ et $\lambda \in \mathbb{R}$. De la même façon,

$$\begin{aligned}\langle (u + \lambda u') \wedge v, w\rangle &= [(u + \lambda u'), v, w] = [u, v, w] + \lambda[u', v, w]\\ &= \langle u \wedge v, w\rangle + \lambda\langle u' \wedge v, w\rangle = \langle u \wedge v + \lambda u' \wedge v, w\rangle\end{aligned}$$

pour tous $u, u', v, w \in E$ et $\lambda \in \mathbb{R}$, ce qui implique que $(u+\lambda u')\wedge v = u\wedge v+\lambda u'\wedge v$ pour tous $u, u', v \in E$ et $\lambda \in \mathbb{R}$. En conséquence, $(u, v) \mapsto u \wedge v$ est une application bilinéaire de E^2 dans E.

(c) (i) On voit bien que

$$\langle u \wedge v, w\rangle = [u, v, w] = -[v, u, w] = -\langle v \wedge u, w\rangle$$

pour tous $u, v, w \in E$, vu que le déterminant est alterné, ce qui implique que $u \wedge v = -v \wedge u$ pour tous $u, v \in E$ et $\lambda \in \mathbb{R}$.

(ii) C'est clair que $0 = [u,v,v] = \langle u \wedge v, v\rangle$ et $0 = [u,v,u] = \langle u \wedge v, u\rangle$, vu que le déterminant est alterné. En conséquence, $u \wedge v$ est orthogonal à u et v.

(iii) On suppose que u et v sont colinéaires. On voit bien que $0 = [u,v,w] = \langle v \wedge u, w\rangle$ pour tous $w \in E$, vu que le déterminant vaut zéro si deux colonnes sont colinéaires. En conséquence, $u \wedge v = \mathbf{0}_E$.

(iv) On suppose que u et v ne sont pas colinéaires. Alors, il existe $w \in E$ tel que $\{u,v,w\}$ est une base de E. En conséquence, $0 \neq [u,v,w] = \langle v \wedge u, w\rangle$, ce qui nous dit que $u \wedge v \neq \mathbf{0}_E$. En plus, $[u,v,u\wedge v] = \langle v \wedge u, u \wedge v\rangle = ||u \wedge v|| > 0$.

(v) On suppose que u et v ne sont pas nuls. Soit $e_1 = ||u||^{-1}u$. Si v et u sont colinéaires, on prend e_2 un vecteur quelconque de norme 1 tel que $\langle e_1, e_2\rangle = 0$. Si $||v||^{-1}v = u$ on prend $\theta = 0$ et si $||v||^{-1}v = -u$ on prend $\theta = \pi$. Par ailleurs, si v et u ne sont pas colinéaires, on considère le sous-espace vectoriel $F \subseteq E$ de dimension 2 engendré par e_1 et v. On prend

$$e_2' = \frac{v - \langle v, e_1\rangle e_1}{||v - \langle v, e_1\rangle e_1||}.$$

Alors, $e_2' \in F$ est un vecteur de norme 1 tel que $\langle e_1, e_2'\rangle = 0$. En plus, comme $||v||^{-1}v$ a norme 1 il existe $(a,b) \in \mathbb{R}^2$ tels que $a^2 + b^2 = 1$ et $||v||^{-1}v = ae_1 + be_2'$. La condition précédente nous dit qu'il existe $\theta' \in]-\pi,\pi]$ tel que $a = \cos(\theta')$ et $b = \sin(\theta')$. si $\theta' \in]-\pi, 0]$, on pose $\theta = -\theta'$ et $e_2' = -e_2$, tandis que si $\theta' \in [0,\pi]$, on pose $\theta = \theta'$ et $e_2' = e_2$. On conclut que $||v||^{-1}v = \cos(\theta)e_1 + \sin(\theta)e_2$.

On voit bien que

$$\begin{aligned}\langle u, v\rangle &= ||u||.||v||\langle ||u||^{-1}u, ||v||^{-1}v\rangle = ||u||.||v||\langle e_1, \cos(\theta)e_1 + \sin(\theta)e_2\rangle \\ &= ||u||.||v||.\cos(\theta)\end{aligned}$$

et

$$\begin{aligned}||u \wedge v|| &= ||u||.||v||.\Big|\Big|(||u||^{-1}u) \wedge (||v||^{-1}v)\Big|\Big| \\ &= ||u||.||v||.\Big|\Big|e_1 \wedge \big(\cos(\theta)e_1 + \sin(\theta)e_2\big)\Big|\Big| \\ &= ||u||.||v||.||e_1 \wedge e_2||.\sin(\theta) = ||u||.||v||.||e_3||.\sin(\theta) = ||u||.||v||.\sin(\theta).\end{aligned}$$

⋆ **26.** Soit E un espace euclidien. Soit u un endomorphisme symétrique positif (*i.e.* $\langle x, u(x)\rangle > 0$ pour tout $x \in E \setminus \{\mathbf{0}_E\}$). On note $\lambda_1, \dots, \lambda_r$ les valeurs propres distinctes de u et $E_1, \dots, E_r$ les sous-espaces propres associés.

(a) Montrer que les valeurs propres de u sont positives.

(b) Montrer que $E_1, \dots, E_r$ sont orthogonaux deux-à-deux et de somme E.

(c) On note $p_1, \dots, p_r : E \to E$ les projecteurs associés à la décomposition d'espaces vectoriels $E = E_1 \oplus \cdots \oplus E_r$. Montrer qu'ils sont symétriques et non négatifs (*i.e.* $\langle x, p_i(x)\rangle \geq 0$ pour tout $x \in E$).

(d) En déduire un endomorphisme symétrique positif dont le carré est u.

(e) Soit v un endomorphisme symétrique positif dont le carré est u. Montrer que v est l'endomorphisme de la question précédente.
Indication : montrer que les E_i sont stables par v, et montrer que les endomorphismes induits sont des homothéties.

Solution. On affirme d'abord que, étant donné un espace de Hilbert $E_{\mathbb{C}}$ de dimension (complexe) finie $n \in \mathbb{N}^*$ muni d'un produit hermitien $b = \langle , \rangle$ et $u_{\mathbb{C}} : E_{\mathbb{C}} \to E_{\mathbb{C}}$ une application $\mathbb{C}$-linéaire hermitienne, les valeurs propres de $u_{\mathbb{C}}$ sont réelles. En effet, si $\lambda \in \mathbb{C}$ est une valeur propre et $x \in \mathsf{Ker}(u_{\mathbb{C}} - \lambda\,\mathsf{id}_{E_{\mathbb{C}}})$ non nul,

$$\bar{\lambda}\langle x,x\rangle = \langle x,u(x)\rangle = \langle u(x),x\rangle = \langle u(x),x\rangle = \lambda\langle x,x\rangle$$

nous dit que $\lambda \in \mathbb{R}$. Soit $u \in \mathsf{L(E)}$ une application symétrique d'un espace euclidien E de dimension finie n. On peut identifier E avec $\mathbb{R}^n$ muni du produit scalaire usuel, on pose $E_{\mathbb{C}} = \mathbb{C}^n$ avec le produit hermitien usuel et $u_{\mathbb{C}}$ est l'unique prolongement $\mathbb{C}$-linéaire de u. Comme u est symétrique, alors $u_{\mathbb{C}}$ est hermitien, ce qui implique que les valeurs propres de $u_{\mathbb{C}}$, *i.e.* les racines dans $\mathbb{C}$ du polynôme caractéristique de u, sont réelles, ce qui implique que les valeurs propres de u coïncident avec celles de $u_{\mathbb{C}}$. En outre, on affirme que u est diagonalisable. Pour le démontrer, soient $\lambda_1,\dots,\lambda_r$ toutes les valeurs propres distinctes de u et $E_1,\dots,E_r$ les sous-espaces propres associés, *i.e.* $E_i = \mathsf{Ker}(u-\lambda_i\,\mathsf{id}_E)$ pour $i \in [\![1,r]\!]$. Il suffit de montrer que $\mathsf{Ker}(u-\lambda_i\,\mathsf{id}_E) = \mathsf{Ker}((u-\lambda_i\,\mathsf{id}_E)^2)$ pour tout $i \in [\![1,r]\!]$. Or, si $w : E \to E$ est une application linéaire, on voit bien que $\mathsf{Ker}(w) = \mathsf{Ker}(w^*w)$. En effet, l'inclusion $\mathsf{Ker}(w) \subseteq \mathsf{Ker}(w^*w)$ est immédiate, tandis que $\mathsf{Ker}(w) \supseteq \mathsf{Ker}(w^*w)$ suit du fait que $w(x) = \mathbf{0}_E$ si et seulement si $\langle x, w^*w(x)\rangle = ||w(x)||^2 = 0$. Comme u est symétrique, $u-\lambda_i\,\mathsf{id}_E$ l'est aussi, ce qui nous dit que $\mathsf{Ker}(u-\lambda_i\,\mathsf{id}_E) = \mathsf{Ker}((u_i-\lambda\,\mathsf{id}_E)^2)$, comme on voulait démontrer.

(a) Soit $\lambda \in \mathbb{R}$ une valeur propre avec vecteur propre $x \in E \setminus \{\mathbf{0}_E\}$, *i.e.* $u(x) = \lambda x$. Alors, $\lambda||x||^2 = \langle v,u(v)\rangle > 0$ nous dit que $\lambda > 0$, vu que u est positif. En conséquence, $\lambda_1,\dots,\lambda_r > 0$.

(b) On rappelle que $E_i = \{x \in E : u(x) = \lambda_i v\}$ pour $i \in [\![1,r]\!]$. Alors, si $x \in E_i$ et $y \in E_j$ avec $i,j \in [\![1,r]\!]$ différents, on a

$$\lambda_i\langle x,y\rangle = \langle u(x),y\rangle = \langle x,u(y)\rangle = \lambda_j\langle x,y\rangle,$$

ce qui implique $\langle x,y\rangle = 0$ car $\lambda_i \neq \lambda_j$. Comme u est diagonalisable, $E = E_1 \oplus \cdots \oplus E_r$.

(c) Comme $\sum_{j=1}^r p_j = \mathsf{id}_E$, on voit bien que

$$\langle p_i(x),y\rangle = \left\langle p_i(x),\sum_{j=1}^r p_j(y)\right\rangle = \langle p_i(x),p_i(y)\rangle = \left\langle \sum_{j=1}^r p_j(y),p_i(y)\right\rangle = \langle x,p_i(y)\rangle,$$

ce qui nous dit que p_i est symétrique pour tout $i \in [\![1,r]\!]$. En outre,

$$\langle x,p_i(x)\rangle = \left\langle \sum_{j=1}^r p_j(x),p_i(x)\right\rangle = \langle p_i(x),p_i(x)\rangle = ||p_i(x)|| \geq 0$$

pour tout $x \in E$ et $i \in [\![1,r]\!]$, ce qui nous dit que p_i est non négatif pour tout $i \in [\![1,r]\!]$.

(d) Soit $\sqrt{u} = \sum_{i=1}^r \sqrt{\lambda_i}p_i \in \mathsf{L}(E)$. Alors $\sqrt{u}\circ\sqrt{u} = u$. En outre, comme la combinaison linéaire réelle d'opérateurs symétriques est symétrique, $\sqrt{u}$ est symétrique. Finalement,

$$\langle x,\sqrt{u}(x)\rangle = \left\langle \sum_{j=1}^r p_j(x),\sum_{i=1}^r \sqrt{\lambda_i}p_i(x)\right\rangle = \sum_{j=1}^r \sqrt{\lambda_i}\langle p_j(x),p_j(x)\rangle = \sum_{j=1}^r \sqrt{\lambda_i}||p_i(x)|| > 0$$

si $x \neq \mathbf{0}_E$, car dans ce cas il existe $i \in [\![1,r]\!]$ tel que $||p_i(x)|| > 0$. En conséquence, $\sqrt{u}$ est positif.

(e) On rappelle que si deux endomorphismes $v,w \in \mathsf{L}(E)$ commutent, alors $w(\mathsf{Ker}(v)) \subseteq \mathsf{Ker}(v)$ et $w(\mathsf{Img}(v)) \subseteq \mathsf{Img}(v)$. En effet, si $x \in \mathsf{Ker}(u)$), alors

$u(w(x)) = w(u(x)) = w(\mathbf{0}_E) = \mathbf{0}_E$, ce qui nous dit que $w(x) \in \mathsf{Ker}(u)$), tandis que $u(w(y)) = w(u(y))$ pour $y \in E$ nous dit que $w(\mathsf{Img}(v)) \subseteq \mathsf{Img}(v)$.

Comme $u = v \circ v$, alors v et u commutent, ce qui implique que $v(E_i) \subseteq E_i$ pour tout $i \in [\![1, r]\!]$. Soit $v_i = v|_{E_i} : E_i \to E_i$. Comme v est symétrique et positive, v_i l'est aussi, et en particulier diagonalisable. Soit $\mathscr{B}_i$ une base de E_i formée des vecteurs propres de v_i. On voit bien que, si $x \in \mathscr{B}_i$ avec valeur propre $\mu > 0$, alors $\lambda_i x = u(x) = v^2(x) = \mu^2 x$, ce qui implique que $\mu = \sqrt{\lambda_i}$. En conséquence, $v_i = \sqrt{\lambda_i}\,\mathsf{id}_{E_i}$ pour tout $i \in [\![1, r]\!]$, ce qui nous dit que $v = \sqrt{u}$, comme on voulait démontrer.